D1.2 – Current state of detection and response to FIMI

1st draft (12 Nov 2024)

Contributors:

Prof. Robert Kupiecki (University of Warsaw)

Prof. Agnieszk Cianciara (ISP PAN)

Prof. Agnieszka Legucka (University of Warsaw)

Amb. Tomasz Chłoń (PORT)

Dr. Filip Bryjka (ISP PAN)

Dr. Katarzyna Golik (ISP PAN)

Sara Nowacka (PhD candidate at ISP PAN)

Paweł Kasprzyk (ISP PAN)

Kamila Szymańska (University of Warsaw)

Methodology and Approach

This report seeks to answer the following question: how the European Union (EU) member states are countering foreign information manipulation and interference (FIMI)? Importantly, the adopted approach is an empirical, and not a normative one. Accordingly, the focus is not on what should be done, but on what is actually being done in the EU member states to counter FIMI. Thus the objective is to conduct a mapping exercise as to where EU member states stand in terms of strategy, policy, institutional capacity, regulation and societal resilience. In turn, this should allow to formulate tentative conclusions as to whether and to what extent a common model for countering FIMI is *de facto* emerging across the EU member states.

Existing research seems to be focused more on operational and normative aspects of countering FIMI, and disinformation more broadly, whereas a comprehensive empirical analysis of strategic, institutional, regulatory, etc. capabilities is still missing, especially when conducted in a broad comparative perspective.

For instance, when discussing strategies to counter disinformation and their effectiveness, authors highlight greater emphasis being put in literature on engaging (responsive) rather than disengaging (alternative) strategies[1]. Whereas the former feature fact-checking, debunking, turning the tables or disrupting the disinformation network and blocking the opponent's messages, the latter rely on prevention campaigns such as educational programmes and various media support initiatives, and legal solutions like speech laws and censorship. However, one must note that the above measures should rather be understood in operational (tactics), rather than strategic terms. In a similar vein, counter-disinformation literature review, conducted by the Global Engagement Centre (GEC) of the US Department of State in July 2023[2], revealed that research on addressing preventative and defensive measures is more prevalent than on punitive or offensive ones. The reviewed literature seems to have predominantly normative orientation, outlining what measures policymakers *should* consider. Accordingly, in terms of defensive measures, policymakers *should* invest in resilience activities, such as fact-checking and media literacy, use a "whole-of-society" approach to detection and monitoring, and emphasize pre-bunking, positive and factual messaging, and amplification. As to offensive measures, policymakers *should* establish standard norms, common definitions, and a formal global code of conduct, pursue timely, targeted, and well-coordinated sanctions, and coordinate with likeminded governments on cyber operations as disinformation responses[3].

In contrast, this report does not aim at providing an exhaustive list of most effective measures to counter FIMI. The report contends that it remains fairly difficult to come up with scientifically rigorous measurement of effectiveness of individual counter-FIMI tactics. Reliance on experts' opinions, which is a tool typically used in think-tank analyses on how to counter disinformation effectively[4], has clear limitations related to normativity, subjectivity

---

[1] Miriam Matejova, Jakub Drmola & Peter Spáč (10 June 2024): Measuring the effectiveness of counter disinformation strategies in the Czech security forces, *European Security*, DOI: 10.1080/09662839.2024.2362153

[2] US Department of State, *Counter-Disinformation Literature Review*, July 2023, https://www.state.gov/counter-disinformation-literature-review/ [last access: 31.10.2024].

[3] Ibidem.

[4] Carnegie Endowment for International Peace, Countering Disinformation Effectively: An Evidence-Based Policy Guide, January 2024, https://carnegieendowment.org/research/2024/01/countering-disinformation-effectively-an-evidence-based-policy-guide?lang=en [last access: 31.10.2024].

and other biases. Thus the authors of this report attach more importance to understanding the actually existing capabilities, coordination mechanisms and cooperation systems implemented across the particular national contexts of EU member states. The authors are convinced that there is no one-size-fit approach and effectiveness should rather be discussed at system-level with proper sensitivity to contextual specificities, and not at the level of individual measures deprived of their political, social and security embeddedness. As a result, it is not the objective of this report to recommend a desirable pre-defined model to be followed by all EU member states, but rather the goal is to highlight both similarities and specificities, areas of convergence and divergence, as well as patterns of diffusion of best practices.

Conceptual approach

The empirical focus does not mean, however, that the report completely abstracts from policy-oriented and actionable conceptualizations of countering FIMI. In fact, various tools oriented towards policy practice have inspired our four-dimension research framework outlined below. One tool worth mentioning is the US Framework to Counter Foreign State Information Manipulation. This framework covers five Key Action Areas[5]: 1) national strategies and policies; 2) governance structures and institutions; 3) human and technical capacity, including digital security tools; 4) civil society, independent media, and academia; and 5) multilateral engagement via multilateral organizations.

The objective of the present report is to adopt a comprehensive and systemic approach to the empirical analysis of EU member states' capabilities in countering FIMI. Accordingly, the research framework features four dimensions to be investigated at member state level:

1) Strategy and policy;
2) Regulatory framework;
3) Institutional capacity;
4) Societal resilience.

One should underline that the framework serves to conduct a mapping exercise rather than a systematic and rigorous comparison across all the 27 EU member states. Both deductive and inductive approaches were used to define specific analytical criteria for each dimension under investigation.

In order to map out national strategies and policies towards countering FIMI we analysed national security strategies, sectoral strategies (mostly related to disinformation, hybrid threats, cybersecurity and digital affairs) and other documents framing policy in this particular area such as action plans, concepts and national frameworks. Comparative analysis of 27 EU member states approaches was followed by detailed analysis of 7 case studies (Netherlands, Latvia, Ireland, Nordics, Czech Republic & Slovakia, Poland & Romania, France) of countries possessing national strategies dedicated to counter disinformation/FIMI or currently processing creation or implementation of such documents.

To analyse the regulation aiming to counter FIMI in EU Member States, we mapped the level of state legal involvement in combating FIMI, categorising legislative approaches ranging from no specific, dedicated regulation to comprehensive FIMI legislation. This was followed by a comparative legal analysis, examining each Member State's approach to FIMI and highlighting their focus on public order, national security and public health. Next, we assessed the role of media and internet regulation, with a particular focus on the EU's Digital Services

[5] US Department of State, The Framework to Counter Foreign State Information Manipulation, January 18, 2024, https://www.state.gov/the-framework-to-counter-foreign-state-information-manipulation/ [last access: 31.10.2024].

Act (DSA), to understand its contribution to the prevention of FIMI and its compatibility with national laws. Finally, we analysed the effectiveness of FIMI regulations to identify best practices and gaps in implementation.

In order to map institutional capacities of EU member states, we sought to investigate processes of institutionalization of national coordination systems, while looking at their centralized or decentralized character, location of the principal coordination mechanism and establishment of specialized state agencies. We sought to investigate usages of analytical framework and digital tools by state institutions. We explored patterns of cooperation between state institutions and non-governmental organizations. Finally, we looked at how institutional best practices are diffused vertically and horizontally, and how they flow from trendsetters to followers.

Methodology

Research methodology included the following techniques: 1) desk research; 2) study visits; 3) expert survey; 4) in-depth expert interviews.

Desk research

Desk research was conducted in line with the four dimensions outlined above and in relation to all 27 member states of the European Union. It was conducted by 8 researchers in total, each responsible for in-depth coverage of three or four member states. Desk research was based on data available in the public domain and reflects the state of art as of 1 July 2024.

Study visits

The research team members participated in three study visits to Vilnius (March 2024),Brussels (April 2024) and Helsinki (October 2024). Group of researchers also participated in Rapid Alert System (RAS) conference organized by Polish MFA and European External Action Service (EEAS) combined with counter FIMI wargame organized by Hybrid CoE in Warsaw (April 2024). Relevant data used for the purpose of this report was obtained during visits to the Lithuanian National Crisis Centre, EEAS, Hybrid Fusion Cell, NATO, Hybrid CoE, among others.

Expert survey

The survey was sent electronically to approximately 150 experts from all the EU member states. We received 32 complete responses. Thus the response rate was at 20%. This relatively low response rate did not come as a surprise due to high level of sensitivity of the topic, and despite the fact that the survey was anonymous. We received at least one response from 18 member states. Whereas not all member states were represented within the sample, we managed to have various geographical regions of the European Union, as well as big and small member states adequately covered.

Number of responses	EU member states represented among respondents
4	Poland Spain
3	Lithuania
2	Bulgaria Germany Italy Malta Portugal Slovakia
1	Belgium Czechia Finland France Greece Hungary Ireland Latvia Netherlands
0	Austria Croatia Cyprus Denmark Estonia Luxemburg Romania Slovenia Sweden

We managed to obtain a fairly balanced response rate in terms of gender: 17 respondents (53%) identified as male, 14 respondents (44%) identified as female, and 1 respondent (3%) preferred not to identify.

In terms of sectoral affiliation the majority of our survey respondents (53%) represented academia and think-tanks. We recorded a sizeable representation of public administration (19%) and non-governmental organizations (16%). Individual respondents came from business, military and media sectors. A relative majority (41%) of respondents declared between 2-5 years of professional experience in the field of countering FIMI. Only 2 respondents declared more than 10 years of professional experience in the field. Female experts had on average less years of professional experience in the field than male experts.

The survey reflected the four-dimension conceptual approach outlined above. Two basic types of questions were asked. The first type of questions aimed at obtaining factual information, notably related to the type of policy documents, state institutions, regulatory acts and non-governmental initiatives that aim at countering FIMI. The second type of questions was about obtaining responder's personal assessment of a given mechanism or tool.

Due to the relatively low response rate we do not analyze survey results separately, nor do we attempt to generate conclusions relying solely on that basis. However, the survey still proved to be a valuable data source insofar as it allowed to triangulate results obtained from desk research and in-depth expert interviews.

In-depth expert interviews

We conducted 22 in-depth interviews with experts from 14 member states. Most of the interviews were conducted online (albeit with some exceptions, with a notable case of French experts). Interviews with experts from a given member state were conducted by a researcher who was in charge of the desk research for this particular member state. Interviews were semi-structured and based on a common pool of questions, adapted to the specificity of the member state, as well as the specificity of the interviewee's expertise. Interviews were not recorded and anonymity was granted to respondents. In addition, the interviews aimed at closing the gaps and triangulating data obtained during the desk research stage.

Number of interviews	**EU member states represented among interviewees**
3	France
2	Czechia Hungary Lithuania Poland Romania Spain
1	Bulgaria Estonia Germany Italy Latvia Portugal Slovenia
0	Austria Belgium Croatia Cyprus Denmark Finland Greece Ireland Luxembourg Malta Netherlands Slovakia Sweden

In contrast to a balanced gender representation among our survey respondents, our interviewees turned out to be mostly men (73%). This was not due to a biased respondent selection, but rather due to the fact that it was predominantly men who agreed to be interviewed.

In terms of sectoral affiliation the relative majority of our interviewees (38%) represented academia and think-tanks. Quite similarly to the survey, we also recorded a sizeable representation of non-governmental organizations (25%) and public administration (21%). Two responders reported double affiliation.

Similarly to the survey, the questions asked during in-depth interviews reflected the four-dimension conceptual approach outlined above. In particular, we wanted to know more about the push factors that led to establishment of particular institutions or entire types of coordination systems, specific regulatory solutions, and modes of cooperation, both nationally (with non-government stakeholders) and internationally (both bilaterally and multilaterally). We also asked our interviewees how they assessed particular institutional and regulatory solutions, or modes of cooperation, and based on what criteria. Finally, we enquired about their informed opinions as to the prospects for development of the counter-FIMI field and community.

Part I – EU'S ROLE IN COUNTERING FIMI

Filip Bryjka, Paweł Kasprzyk

1.1. Evolution of disinformation to FIMI concept

FIMI is a growing political and security challenge highlighting the need for a common defence framework. The FIMI concept permits EEAS to maintain situational awareness of developments in the information space without limiting its monitoring and analysis function to specific actors. Instead, it sets out best practices for fighting disinformation through sharing data and analysis, and can inform effective action. Adopting a whole-of-society approach will be needed to enhance resilience and leverage the broadest capacities and competencies. However, this can be realistically achieved only if the large variety of actors engaged in countering FIMI speak a common language.[6]

Between 2015 and 2021, in the context of information manipulation EU used the definition of **disinformation** understood as a "verifiably false or misleading information that is created, presented, and disseminated for economic gain or to intentionally deceive the public, and may cause public harm"[7]. The category of **foreign information manipulation and interference (FIMI)** was introduced into the official language of the EU in March 2022. It is a broader concept than disinformation and describes "a mostly non-illegal pattern of behaviour that threatens or has the potential to negatively impact values, procedures, and political processes. Such activity is manipulative in character, conducted in an intentional and coordinated manner, by state or non-state actors, including their proxies inside and outside of their own territory"[8].

Accordingly, FIMI is set apart from misinformation and disinformation. Unlike in the case of misinformation, it is spread intentionally to deceive the public and FIMI does not refer solely to false or misleading information, unlike disinformation. This latter aspect of the concept is a welcome evolution as malicious actors have long understood that the best influence operations are not simply limited to false information. As pointed out by the EU DisinfoLab:

---

[6] To help operationalise the concept, the EEAS recommends following a Kill Chain taxonomy of FIMI TTPs developed by the Disinformation Analysis and Risk Management (DISARM). It sets out best practices for fighting disinformation through sharing data & analysis, and can inform effective action.
European Union External Action Service (EEAS). *1st EEAS Report on Foreign Information Manipulation and Interference Threats - Towards a framework for networked defence,* p. 29–30.

[7] European Commission. 2018. "Tackling online disinformation: A European Approach. COM(2018) 236 Final." https://eur-lex.europa. eu/legal-content/EN/TXT/?uri=CELEXper cent3A52018DC0236.

[8] European External Action Service (EEAS). October 2021. "Tackling Disinformation, Foreign Information Manipulation and Interference. Stratcom Activity Report." https://www.eeas.europa.eu /eeas/2021-stratcom-activity-report-strategic-communication-task-forces-andinformation-analysis_en.

"*not all disinformation is FIMI, and FIMI is not only disinformation.*"[9] The main nuances between the concepts of FIMI and disinformation are:

- a refocusing of interest on behaviour and operating methods (while counter-disinformation activities often look at the content and tackling of narratives);
- increased use of terms and processes from cyber-threat intelligence (enabling us to expand the toolbox of countermeasures beyond the current focus on strategic communication and debunking of misleading or false narratives);[10]
- a holistic approach mobilising whole-of-society's resources, favouring the adoption of common terminology.

Thus, on the one hand FIMI can be perceived as a narrower concept from disinformation because it refers to foreign activity alone, leaving out domestically grown activities. On the other hand it should also be perceived as wider as it does not limit itself to false or misleading information. Instead, the focus is on the manipulative behaviour exhibited in the process of delivering the information, such as an artificial amplification of a narrative through fake social media accounts thereby influencing a public debate.[11]

The concept of FIMI is increasingly used across the EU and its Member States. The origins of the concept may be traced to 2019,[12] when the issue of foreign digital interference and the potential benefits of standardising the description of observed incidents and the terminology came to the attention of the EEAS. The concept was further developed in two other EU official documents key to the evolution of the concept: the December 2020 *European Democracy Action Plan*[13] and the 2022 *Strategic Compass,*[14] which called for the development of an EU FIMI-dedicated toolbox. The doctrinal evolution concludes with the first EEAS report on *Foreign Information Manipulation and Interference Threats* from February 2023.[15]

According to the EEAS definition, FIMI operators "can be state or non-state actors, including their proxies inside and outside of their own territory."[16] Therefore, the analytical framework

---

[9] N. Hénin. *FIMI: towards a European redefinition of foreign interference.* EU Disinfo Lab, 1–11. https://www.disinfo.eu/wp-content/uploads/2023/04/20230412_FIMI-FS-FINAL.pdf [date published: 07.04.2023], p. 4.

[10] The EEAS FIMI framework builds on experience in cybersecurity, where the forensic analysis focuses on threat actor behaviour throughout the entire timeline of their attempted attack (the so-called "Kill Chain" model) has helped to better understand systemic vulnerabilities, and how to spot and close their exploitation.At the heart of the Kill Chain perspective on FIMI is the systematic and granular data collection on "Tactics, Techniques, and Procedures' (TTPs) which are patterns of behaviour used by threat actors to manipulate the information environment with the intention to deceive. This method allows us to ask what a threat actor was doing before they were able to deploy a message; where in the attack chain they are currently and what their next step(s) may be, Ibidem, p. 9.
European Union External Action Service (EEAS). *1st EEAS Report on Foreign Information Manipulation and Interference Threats - Towards a framework for networked defence*, p .4.

[11] European Union External Action Service (EEAS). *1st EEAS Report on Foreign Information Manipulation and Interference Threats - Towards a framework for networked defence,* p. 25.

[12] Hénin. *FIMI: towards a European redefinition of foreign interference,* p. 4.

[13] European Commission. *Communication from the commission to the European Parliament, The Council, The European Economic and Social Committee and The Committee of the Regions on The European Democracy Action Plan.*

[14] European Union External Action Service (EEAS). *A Strategic Compass for Security and Defence*, 1–64. https://www.eeas.europa.eu/sites/default/files/documents/strategic_compass_en3_web.pdf [date published: 24.03.2022], p. 12, 40.

[15] European Union External Action Service (EEAS). *1st EEAS Report on Foreign Information Manipulation and Interference Threats - Towards a framework for networked defence*.

[16] Ibidem, p. 4.

is applicable to all regions and actors as well as foreign and domestic analyses for its actor-agnostic design. Hence, it may be used by all stakeholders regardless of their respective focus.[17] Member States can adapt the framework according to their own analytical limitations and institutional division of competences concerning either domestic or foreign actors.

The approach offered by the EEAS focuses on behaviour rather than content (narrative) or the actor involved. Importantly, the focus on behaviour enables expanding the toolbox of countermeasures beyond strategic communication and debunking of misleading or false narratives. It helps to alleviate some of the institutional difficulties in engaging with content, which is highly political by nature, such as allowing the EEAS to avoid accusations of censorship or authoritative decision-making on what is true or false.

EU Member States have not established uniform criteria to qualify information incidents as FIMI. Similarities in approach can however be observed among some of the leading nations. For example the Swedes consider a FIMI incident to: 1) have a foreign origin; 2) contain content that misleads the recipient; 3) have the intent to inflict harm; and 4) carry potential security risks[18] while the French agency VIGINUM considers similar criteria for digital interference: 1) involvement of foreign actors; 2) inauthenticity of behaviour; 3) misleading content; and 4) specific target[19]. The experts who took part in the survey for this project indicated that the main factors that make a FIMI incident relevant for further analysis or reaction are:

- Attack on the fundamental interests of the state (87,5%)
- Manifestly inaccurate or misleading content (71,8%)
- Inauthentic distribution of content (65,6%)
- Automated distribution of content (46,8%).

2.1. The impact of new technologies to evolution of FIMI

The conceptual framework of FIMI is not limited to fake news, propaganda, or disinformation, but focuses on interference in the political processes of states subjected to hostile information influence. It covers the problem of information manipulation more broadly by taking into account the evolving tactics, techniques and procedures (TTPs) used by Russia, China, and Belarus, among others, including in the cyber domain (e.g., attacks on voter registries, deep fakes, or hack-and-leak operations involving the stealing and publishing of confidential information or correspondence). To counter FIMI, EU states are adopting new strategies and policies, creating dedicated structures in public administration, improving the regulatory framework as well as engaging civil society organisations and cooperating with online platforms and the media. In doing so, they must constantly adapt to the changing TTPs used by threat actors.

FIMI operations are characterised by increasing levels of automation due to technological advances. Using bot farms — computer programs that mimic human online behaviour — attackers spread manipulated content on a massive scale and increase the reach of malicious activity. A common method is to impersonate politicians or institutions by cloning their websites and official social media accounts. FIMI operations are carried out with the help of sophisticated infrastructure and cloaking software, making it difficult to detect the attacker and attribute responsibility. The use of artificial intelligence (AI) is playing a growing role in

[17] States remain central FIMI threat actors. Moreover, the EEAS admits that its mandate and strategic priorities have limited the focus on influence operations conducted by two state actors, namely Russia and China. Ibidem, p. 8.
[18] Based on the Swedish presentation at the RAS PoCs conference in Warsaw, 9-12 April 2024.
[19] Based on the French presentation at the RAS PoCs conference in Warsaw, 9-12 April 2024.

FIMI operations, enabling to create fake but authentic appearing social media personas en masse, or fake speech by a real person (deep fake)[20]. For example the U.S. Federal Bureau of Investigation (FBI) and Cyber National Mission Force (CNMF), in partnership with the Netherlands General Intelligence and Security Service (AIVD), Netherlands Military Intelligence and Security Service (MIVD), the Netherlands Police (DNP), and the Canadian Centre for Cyber Security (CCCS), have found that Russian state-sponsored actors (RT affiliates) used an AI enhanced software package (Meliorator) to create fictitious online personas, representing a number of nationalities, to post content on X (formerly Twitter)[21]. The software was used for foreign malign influence activity benefiting the Russian government. Using this tool, RT affiliates disseminated disinformation to and about a number of countries, including the United States, Poland, Germany, the Netherlands, Spain, Ukraine, and Israel[22].

The use of AI in information operations is leading to a situation in which actors who are able to master the technology and are willing to deploy it in a deceitful fashion are gaining influence over the outcome of elections in democratic states. New technologies and cyberspace are used with malign intent to design and execute influence operations targeting mass audiences and specific communities. They provide an advantage, as they enable the distribution of manipulated content on a mass scale without the attacker ever having to suffer meaningful consequences for such activity. The threat is likely to increase in the future as AI-based technology will be able to plan even entire campaigns (including determining narratives and target groups).

AI-based tools are being developed at a far higher pace then the ability of state authorities to regulate them. Furthermore, significant differences in capability levels exist between EU Member States and their ability to enforce regulation vis-a-vis online platforms, as well as between Europe itself and the US.

In addition to improving the implementation of the EUs Digital Services Act (DSA), Media Freedom Act and the AI Act, the counter FIMI advocacy community should prioritise efforts to develop tools for bot, deep fakes and other inauthentic behaviour detection. The tools currently available are insufficient. The use of AI in countering FIMI should also be explored more pro-actively. According to results of recent studies the ability of AI algorithms to persuade humans is predicted to exceed 90% in the next few years. A study published by „Science Magazine" indicates that tools such as chatbots can be used, for example, to disprove conspiracy theories. After a nine-minute conversation with a bot, 20% of conspiracy theorists stopped believing them altogether and 27% began to doubt them.[23]

Due to the role of new technologies cooperation with the private sector plays a key role in countering FIMI. In **September 2018, the Union adopted the "Code of Practice"** governing EU countries' cooperation with the private sector (including major online platforms

---

[20] Nicolas Mazzucchi, *AI-based technologies in hybrid conflict: The future of influence operations*, Hybrid CoE Paper, no. 14, June 2022, p. 6.

[21] Although the tool was only identified on X, the authoring organizations' analysis of Meliorator indicated the developers intended to expand its functionality to other social media platforms. The authoring organizations' analysis also indicated the tool is capable of the following: creating authentic appearing social media personas en masse; deploying content similar to typical social media users; mirroring disinformation of other bot personas; perpetuating the use of pre-existing false narratives to amplify malign foreign influence; and formulating messages, to include the topic and framing, based on the specific archetype of the bot.

[22] *State-Sponsored Russian Media Leverages Meliorator Software for Foreign Malign Influence Activity*, Joint Cybesecuriry Advisory, 09.07.2024.

[23] Thomas H. Costello, Gordon Pennycook, David G. Rand, *Durably reducing conspiracy beliefs through dialogues with AI*, „Science", Vol 385, Issue 6714, 3 Sep 2024 DOI: 10.1126/science.adq1814

such as Facebook, Google, Twitter, Mozilla, and Microsoft) on obligations for online platforms and the advertising industry to improve the transparency of political advertising, take down fake accounts, and reduce incentives to spread disinformation. In **2022, the Code was updated** and was signed by 34 private entities. The Strengthened Code of Practice on Disinformation brings together a more diverse range of stakeholders than ever, empowering them to contribute to wide-ranging improvements by signing up to precise commitments relevant to their field. Such commitments include demonetising the dissemination of disinformation, guaranteeing the transparency of political advertising, enhancing cooperation with fact-checkers, and facilitating researchers' access to data[24]. The code sets broad commitments and measures to counter online disinformation for its voluntary signatories, from fact-checking and advertising industries, to researchers and civil society representatives. These measures include demonetising the dissemination of disinformation, securing the transparency of political advertising and providing researchers better access to data. Disinformation and foreign interference are also dealt with within the hybrid threats framework.[25]

Many believe that a breakthrough in the fight against disinformation has been achieved with the adoption in 2022 of the **Digital Services Act (DSA),** EU's landmark regulation entered into full effect in February 2024, created binding obligations for very large online platforms and search engines to counter illegal online content. It also established transparency and oversight measures and rules for content moderation. These rules aim to safeguard fundamental rights of online users and establish accountability to mitigate systemic risks such as disinformation or election manipulation. For the first time, the DSA provides a uniform legal framework across the EU to counter risks related to disinformation and foreign interference[26]. Once fully implemented by the EU Member States, the DSA will be the world's first regulation bringing transparency and public oversight of very large online platforms and search engines. The EU hopes that the DSA will become a model for similar legislation in other parts of the world[27].

The EU has also established measures to protect the freedom of media and ensure the independent functioning of public service media. In March 2024, the EU introduced its new Media Freedom Act that obliges Member States to to protect journalists and media independence against political or economic interference.[28] The Act also establishes responsibilities on the media on transparency of ownership and state advertising funds. Other EU policies and action plans to respond to and build resilience against foreign information manipulation include the 2024 Artificial Intelligence Act[29] for regulating the risks of AI and the Defence of Democracy package, adopted ahead of the European Parliament election in June 2024 to enhance transparency and accountability through legislative and non-legislative

---

[24] *Strengthened Code of Practice on Disinformation 2022*, European Commission, 16 June 2022, www.digital-strategy.ec.europa.eu.
[25] European Commission. *The 2022 Code of Practice on Disinformation.* https://digital-strategy.ec.europa.eu/en/policies/code-practice-disinformation [date published: 24.4.2024].
[26] European Commission. *Questions and answers on the Digital Services Act.* https://ec.europa.eu/commission/presscorner/detail/en/QANDA_20_2348 [date published: 23.2.2024].
European Commission. *The Digital Services Act package.* https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package [date published: 16.2.2024].
[27] M. Makowska, *EU Agrees the Digital Services Act*, "PISM Bulletin", 16 May 2022, www.pism.pl.
[28] European Commission. *European Media Freedom Act.* https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/new-push-european-democracy/protecting-democracy/european-media-freedom-act_en [date published:15.03.2024].
[29] European Parliament. *Artificial Intelligence Act,* (P9_TA(2024)0138). https://www.europarl.europa.eu/doceo/document/TA-9-2024-0138_EN.pdf [date published: 13.03.2024].

measures to tackle the threat of covert foreign influence in democratic processes. It also encourages citizens and civil society organisations to participate in building civil resilience.[30]

3. EU's approach to counter FIMI

The Strategic Compass, adopted by the EU Council on 21 March 2022, less than a month after the Russian invasion of Ukraine, proposed to increase the resilience of states and societies to foreign information manipulation and interference by developing a counter FIMI Toolbox. In recent years, the European Union has established many instruments that enable institutions and Member States to address FIMI, while fully respecting fundamental rights and freedoms. The FIMI Toolbox outlines different areas and instruments that together constitute a robust and comprehensive framework for tackling FIMI. The toolbox includes short-, medium- and long-term measures – from prevention to reaction – and it is a dynamic system in order to account for the constant evolution of the threat. The envisaged instruments have been grouped into four dimensions:

1. **Situational Awareness** – a thorough understanding of the threat is a key prerequisite, to inform which response and which responder are most appropriate.
2. **Resilience Building** – examples include strategic communication, cooperation within the EU's Rapid Alert System (RAS) or efforts to inform and raise awareness.
3. **Disruption and Regulation** – efforts to further trust, transparency and safety in the information environment, such as the Digital Services Act, are permanent instruments that shape the environment in which responses to FIMI are taken.
4. **Related to EU external action including Common Foreign and Security Policy (CFSP) and diplomatic responses** – this dimension makes use of instruments in the area of foreign and security policy, such as international cooperation, the G7 Rapid Response Mechanism or sanctions such as those imposed on Kremlin-controlled outlets like RT and Sputnik[31].

Table 1: Foreign Information Manipulation and Interference Toolbox

Situational Awareness	Resilience Building	Disruption & Regulation	EU External Action
Common Framework & Methodology	Strategic Communication	Digital Service Act	Restrictive Measures
Monitoring & Detection	Policy Responses and Strategy	Code of Practice on Disinformation	Political Attribution
OSINT Investigations	Internal Organizational Structures	European Media Freedom Act	International Norms and Principles
Information Sharing & Analysis	Rapid Alert System	Transparency	Diplomatic Responses
Impact Assessment	Awareness Raising and Exposure	Addressing AI and Emerging Technologies	G7 Rapid Response Mechanism and others
	Capacity Building	Other Legislation and Regulation	International and Multilateral Cooperation
	Digital, Media and Information Literacy	Engaging with the Private Sector	
	Strengthening Independent Media		
	Empowering Civil Society		

[30] European Commission. *Defence of Democracy – Commission proposes to shed light on covert foreign influence.* https://ec.europa.eu/commission/presscorner/detail/en/ip_23_6453 [date published: 12.12.2023].
[31] *2nd EEAS Report on Foreign Information Manipulation and Interference Threats: A Framework for Networked Defence*, European External Action Service, Brussels, January 2024, p. 14.

	Fact-Checking		

Source: *2nd EEAS Report on Foreign Information Manipulation and Interference Threats: A Framework for Networked Defence*, European External Action Service, Brussels, January 2024, p. 13.

Situational awareness of the threat is key to early detection and appropriate response. Documenting the threat – sufficiently and systematically enough – is our first (1) line of defence against FIMI. Being informed is necessary step to go further: (2) raise the awareness about the threat among various audiences (decision makers, media, society, etc.); (3) repairing the weaknesses that the aggressors exploit (e.g. by introducing media literacy programs, pressure on internet platforms to prevent manipulation operations); (4) punish the aggressors by limiting threat actors capabilities to operate (e.g. imposing sanctions or blocking domains)[32].

Russia's illegal annexation of Crimea in 2014 and disinformation campaigns in the Member States compelled EU institutions to build up special mechanisms and tools to better detect and deter FIMI operations. In March 2015, the European Council asked the High Representative for Foreign Affairs and Security Policy to develop an action plan for strategic communications to counter Russia's disinformation campaigns. As a result, a task force responsible for monitoring, analysing, and responding to Russian propaganda and disinformation, **East StratCom, was established within the European External Action Service (EEAS)**. In 2017, two further StratCom task force units were created: one for the Southern Neighbourhood (South StratCom Task Force) and one for the Western Balkans (Western Balkans Task Force). A Sub-Saharan Africa StratCom task force was finally added in 2024.

These teams are part of the **40 or so-strong Strategic Communications, Task Forces, and Information Analysis Division at the EEAS**[33], which supports EU institutions with policy planning, strategy, and strategic communication tools. It also provides support (e.g., analysis and instructions to combat disinformation) for EU delegations, missions and operations under the Common Security and Defence Policy (CSDP). The unit also develops cooperation with partner countries, the G7, NATO, civil society organisations, and the private sector (e.g., on data acquisition using modern software and technology). The aim of these activities is to build public awareness and strengthen resilience to disinformation[34].

To increase the situational awareness of hostile information manipulation, in March 2019 the Union established the **Rapid Alert System (RAS)** on Disinformation. The exchange of information under this system takes place through points of contact (PoCs) established in

---

[32] Jakub Kalenský, *The structure and the effect of the disinformation ecosystem*, Information Security Summit IS2, https://is2.cz/en/articles/speakers-2020/jakub-kalensky-en [09.09.2024]

[33] Russia's full-scale invasion of Ukraine intensified the activities of EU institutions in countering disinformation. East StratCom has been strengthened financially and in staffing. It now has 13 full-time employees who can outsource research tasks and analyse how Russia adapts its disinformation techniques and methods to changing situations. East StratCom monitors information messages published in more than 20 languages. Therefore, within the EEAS, similar tasks to East StratCom are carried out by analogous teams (six full-time staff each) responsible for the Western Balkans region and the Middle East and North Africa. They focus on counter-radicalisation, combating propaganda from terrorist organisations as well as disinformation from Russia, China, Iran, and Turkey. In addition, there is a Horizontal Threat Team dealing with Chinese disinformation (four staff members), a team supporting EU missions and operations, a team analysing quantitative data on disinformation techniques, tactics, and procedures (TTPs) used by disinformation actors (three analysts), and two political action teams dealing with building resilience. As a result of French advocacy it has been created a team responsible for Sub-Saharan Africa, which is now seen as the main focus of Russian disinformation operations. Based on interviews with EEAS staff, conducted on 21 June 2023 in Warsaw.

[34] *2021 StratCom activity report - Strategic Communication Task Forces and Information Analysis Division*, 24 March 2022, www.eeas.europa.eu.

individual Union countries. The persons acting as PoCs in the RAS in the Member States come mainly from the StratCom units within the Ministry of Foreign Affairs (MFA), the Ministry of the Interior (MOI) and the Ministry of Defence (MOD). The system was used in 2020 during the COVID-19 pandemic when the information space was flooded by a wave of Russian and Chinese disinformation undermining confidence in Western vaccines (mainly mRNA-type), EU institutions, and vaccination strategies, and fuelling anti-vaccination movements[35]. The system was used to exchange information between EU institutions and the Member States, private sector representatives, and G7 and NATO members. However, these actions did not stop the wave of conspiracy theories spread by, among others, anti-vaccine circles or pro-Russia and pro-China news channels (including "troll factories").

RAS ias an platform for the exchange of information between PoCs has some limitations and drawbacks that affect its functioning. One dysfunctionality is that PoCs only receive incident information when they are logged into the system. In a situation where a PoC is in a business meeting/trip, or is carrying out other tasks that prevent him or her from logging into the system, de facto is not able to be informed about the alert, which can delay the reaction[36]. Therfore, alternative (informal) system of warning should be applied.

In the assessment of RAS users not all incidents are important enough to put in the system.They should inform each other about identified incidents that:

(i) may lead to the triggering of socio-political actions (e.g. protests, demonstrations, riots, etc.);
(ii) may be part of a larger operation carried out on the territory of several EU countries;
(iii) are carried out in a combination of cyber-attacks, e.g. on state electoral commissions.

Users of the system also stressed that it would be useful for Member States to share technical reports of their investigations, which can help to detect operations carried out in other EU countries, as well as attribute attribution to the attacker[37]. Until now, Member States are not willing to share such detailed reports. An exception that could be a turning point is the publications of the French VIGINUM titled 'Portal Kombat' exposing the activity of a network of 193 'information portals' with similar characteristics, disseminating pro-Russian content and targeting several western countries (including France, Germany, Austria, Switzerland, Poland, United Kingdom, and the United States)[38]. It's going public contributed to the removal of the network of Telegram accounts linked to these webisites that were used by Russia in the operation aimd at distortion of Western public perception of the Russian invasion of Ukraine.

Although RAS is a platform of state-state information exchange, **Foreign Information Manipulation and Interference Information Sharing and Analysis Center (FIMI-ISAC)** is a group of like-minded organisations that protect democratic societies, institutions, and the critical information infrastructures of democracy from external manipulation and harm. Through collaboration, the FIMI-ISAC enables its members to detect, analyse, and counter FIMI more rapidly and effectively while upholding the fundamental value of freedom of

---

[35] A. Legucka, M. Przychodniak, *Disinformation from China and Russia during the COVID-19 Pandemic*," PISM Bulletin, No, 86, 21 April 2020, https://www.pism.pl/publications/Disinformation_from_China_and_Russia__during_the_COVID19_Pandemic

[36] Based on the discussion held during RAS PoCs conference in Warsaw, 9-12 April 2024.

[37] Based on the discussion held during RAS PoCs conference in Warsaw, 9-12 April 2024.

[38] *Portal Kombat. A structured and coordinated pro-Russian propaganda network. Technical report*, VIGINUM, February 2024.

expression. The FIMI-ISAC does not act independently to counter FIMI. Instead, enhancing collaboration empowers its members to do so more effectively[39].

3. Standardisation of FIMI detection and response

Like in cases of other hybrid threats, responsibility for countering FIMI is the responsibility of the Member States. However, the effectiveness of these activities depends on the cooperation of various countries and organisations. Institutions responsible for countering FIMI in EU countries are located in different government structures (e.g., foreign affairs, interior, defence ministries) by which they have different mandates, organisation, and scope of tasks. They also use different methodologies for analysing FIMI incidents, which makes it difficult to share information. Therefore, since 2015 the EU is developing its own capabilities to monitor, identify and analyse disinformation, as well as to enable the exchange of information between member states and like-minded partners. Delivering on the commitments made under the Strategic Compass, as well as in line with objectives of the European Democracy Action Plan , the EU focused on responding to the following main needs:

1. A common terminology to establish a common understanding of the threat and to facilitate whole-of-society collaboration;
2. A common framework to optimise knowledge generation, exchange and activation based on open-source and collaborative standards;
3. An EU Toolbox of joint responses (FIMI Toolbox) to inform effective and proportional counter-FIMI measures[40].

Since the adoption of the Strategic Compass in March 2022. The EU aims to standardise the detection and response to FIMI based on the DISARM-STIX[41] method, used, among others, by the Data Analysis Team in the Strategic Communications, Task Forces and Information Analysis Division (SG.STRAT.2) of the EEAS. This method allows, among other things, the analysis of tactics, techniques and procedures used, as well as information on the infrastructure used to carry out influence operations (e.g., domains, servers, inauthentic accounts, etc.) to be entered into a common database.

The EEAS's conceptual work has led it to propose a common analytical framework and methodological standards, which, although not mandatory for EU countries, are widely considered best practice. It is up to individual Member States to decide on their possible implementation. Further standardisation of working methods by EU governments' analysts in, as well as NGOs involved in combating FIMI, would greatly enhance the situational awareness of Member States and improve the exchange of information among them.

However, the results of our survey indicate that there is still a low uptake of EU standards by Member State. The most popular framework for analysing TTPs by state institutions is DISARM, whose use was declared by 28.1 % of respondents. Open CTI, a tool for collecting and exchanging data on analysed FIMI incidents, is used by 21.8 % of them, while the STIX format is used by 15.6 %. The lowest rate of positive responses was achieved by the ABCDE framework (only 6.25%), which de facto includes the comprehensive use of DISARM and STIX using Open CTI. Nearly a fifth (18.75%) indicated that they use other analytical tools.

---

[39] *FIMI-ISAC Collective Findings I: Elections*, October 2024, https://fimi-isac.org/wp-content/uploads/2024/10/FIMI-ISAC-Collective-Findings-I-Elections.pdf

[40] *2nd EEAS Report on Foreign Information Manipulation and Interference Threats: A Framework for Networked Defence*, European External Action Service, Brussels, January 2024, p. 12.

[41] H. Newman, *Foreign information manipulation and interference defence standards: Test for rapid adoption of the common language and framework 'DISARM'*, Hybrid CoE Research Report 7, November 2022.

The results look different in NGOs involved in the detection and analysis of FIMI. First of all, it is important to note the high rate of use of the ABCDE and DISARM framework (22.4%), indicating the integral use of both. However, the STIX format and the Open CTI software scored worse (12.5% in both cases) compering to government institutions, which may indicate insufficient involvement of NGOs in information sharing.

	State institutions	NGOs
ABCDE	6,25%	22,4%
DISARM	28,1%	22,4%
STIX	15,6%	12,5%
Open CTI	21,8%	12,5%
Other	18,75%	18,75

Source: own study (survey)

Standardisation of FIMI analysis methods would also facilitate technical attribution of FIMI incidents. This, in turn, should improve decision-making at the political level regarding joint (coordinated) responses. The ability to attribute responsibility for an attack is also an essential element of deterrence, as it imposes costs on the aggressor, ranging from image and credibility to political, and even financial if sanctions are imposed.

The 2nd EEAS report on FIMI proposed a "FIMI Response Framework" with the „aim of linking analysis and insights even more effectively to timely responses, highlighting the importance of cooperation between all the stakeholders that hold key instruments to respond to the intentional manipulation of the information environment"[42]. The Framework is a guide to how defenders can prevent, prepare for, respond to and recover from FIMI attacks while continuously improving their security in future attacks. The Framework is composed of three main elements:

1) *Cross-domain analysis* – integration of FIMI analysis with other data sources of analysis (with the use of OSINT, ABCDE, DISARM, STIX frameworks among others).
2) *Adapted countermeasures* – pre-identication of responses based on the attack pattern (identified TTPs) and activation time:
    a. Pre-incident (preventive counters)
        i. Creation of common Analytical Frameworks and Methodology
        ii. Implementation of programmes of Media and Information Literacy, support for Independent Media, support to Civil Society and support to Fact Checking initiatives
        iii. Use of Strategic Communication activities to build resilience and trust
        iv. Investment in Capacity Building to enable members of the defender community
        v. Creation of policy instruments (like the AI Act, Code of Practice on Disinformation or the Digital Services Act)
    b. Mid-incident (reactive counters)
        i. *Ignore* – sometimes it's better to ignore an incident than to react to it, which can lead to publicised manipulation and be counter-productive
        ii. *Contain* - inform online platforms when an inauthentic network or harmful content is detected
            a. Pre-bunk a story before it strikes
            b. Early exposure of a network

[42] *2nd EEAS Report on Foreign Information Manipulation and Interference Threats: A Framework for Networked Defence*, European External Action Service, Brussels, January 2024, p. 5.

c. Rapidly inform stakeholders of your findings to active contingency plans
d. Restrict amplification of manipulated content
e. Prompt audiences when they engage with a manipulated content

iii. *Minimise* – remove inauthentic accounts and the content they distribute
a. Remove content violating pre-existing community guidelines: coordinated and inauthentic behaviour, impersonations, malicious false content, nontransparent paid ads.
b. Remove or transfer websites, channels or accounts involved in FIMI activities
c. Issue legal notices

iv. *Redirect* – redirect the recipient's attention to reliable information with a message at the appropriate level.
a. Expose and debunk the incident, manipulation techniques and threat actor objectives
b. Provide suitable, easily accessible, reliable information
c. Update and adapt misused content to redirect audiences to verified content
d. Use humour-based responses
e. Label false and misleading content with warnings or debunks by third-party organisations
f. Give visibility to reliable content

c. Post-incident (adaptive counters)
i. Information sharing with relevant stakeholders to reinforce situational awareness
ii. Capacity building among the defender community, based on insights gained from previous incidents
iii. Identify and limit financial incentives for FIMI activities
iv. Activate diplomatic responses
v. Deploy legal responses, including sanctions
vi. Monitor and respond to evasion tactics circumventing legal responses
vii. Reinforce and adapt response instruments based on lessons learnt

3) *Mechanisms for collective response* – increased community collaboration and protocols to activate responses[43].

4. Disruption of FIMI by sanctioning threat actors

After the full-scale invasion of Ukraine in February 2022, Russian media were finally recognised by the EU as tools of warfare on the information front. In March, the Council of the European Union imposed sanctions on Russian state broadcaster RT/Russia Today and the Sputnik agency (including their various language versions)[44]. For years, they have been among the main tools of Russia's ecosystem of disinformation and propaganda against Ukraine and Western countries. These media are under the direct or indirect permanent control of the Russian authorities and used to support unjustified armed aggression against

[43] *2nd EEAS Report on Foreign Information Manipulation and Interference Threats: A Framework for Networked Defence*, European External Action Service, Brussels, January 2024, p. 15-18.

[44] These are RT, formerly Russia Today, and its affiliates, including Russia Today English, Russia Today UK, Russia Today Germany, RT Balkans, Russia Today France, Russia Today Spanish, and RT Arabic, as well as Sputnik and its affiliates, including Sputnik Arabic. In June 2023, Oriental Review, Tsargrad, New Eastern Outlook and Katehon were further restricted as part of the 11th sanctions package.

Ukraine and to destabilise neighbouring countries. They also constitute a serious and immediate threat to public order and security in the European Union[45].

After 24 February, leading Russian propagandists, including TV presenter Vladimir Solovyov and editor-in-chief of the English-language version of RT, Margarita Simonyan, were placed on the EU sanctions list. In total, more than 50 propagandists from the Kremlin and other entities involved in Russian disinformation activities have been included on the list, including Rossiya RTR/RTR Planieta, Rossiya 24/Russia 24, Rossiya 1, TV Centre International, NTW/NTV Mir, REN TW, Pervy Kanal, and the media organisation RIA FAN, with more being added in subsequent sanctions packages. The restrictions imposed by the EU prevent these media from broadcasting material via cable and satellite, as well as transmitting (via web TV, platforms, portals, and apps) content that undermines the democratic order in European countries and aims to polarise EU societies. However, the Council's decision was temporary. The sanctions were put in place "until the aggression against Ukraine ceases and the Russian Federation and its associated media cease their disinformation and manipulative activities against the EU and its Member States"[46].

June 2024 EU 14 sanctions package against Russia, including new restrictions on Russian funding of political parties and other 'opinion forming' organisations and Russian state media in the EU. The new EU sanctions package prohibits EU entities that are 'part of the opinion-forming process', including political parties, foundations, alliances, NGOs, think tanks and media providers in the EU from accepting donations, funding or other economic benefits or support 'from Russia, directly or indirectly'[47]. The EU cites Russia's ongoing propaganda and disinformation campaigns aimed at undermining Ukraine's sovereignty and independence, justifying the war in Ukraine and influencing democratic processes in the EU as the reason for this particular restriction. The EU sanctions regulation defines these Russian 'direct and indirect' actors vaguely as 'Russia and its proxies'[48]. The EU also implemented a decision it adopted on 17 May to 'suspend the broadcasting activities of additional media outlets in the Union or directed at the Union', including the explicitly Kremlin-owned news services and depots RIA Novosti, Izvestia, Rossiskaja Gazeta and Voice of Europe[49], until 'Russian aggression in Ukraine is ended' and until Russia 'and its affiliated media outlets cease their propaganda activities' in the EU. The EU defines sanctioned entities as 'media under the permanent direct or indirect control of the [Russian] leadership' and whose propaganda activities 'support Russia's war of aggression against Ukraine' and 'destroy' Ukraine's neighbouring countries. countries neighbouring Ukraine. The EU decision notes that the rules apply only to the 'broadcasting activities' of the organisations concerned and do not impede journalists from conducting interviews and research in EU member states. From 2022. The EU has suspended the 'broadcasting activities and licences' of 18 Kremlin-backed disinformation stations. The EU does not define what constitutes 'broadcasting activity' in the

[45] For more extensive information about the role of RT and Sputnik in the Russian disinformation-propaganda ecosystem, see: U.S. Department of State, "GEC Special Report: Kremlin-Funded Media: RT and Sputnik's Role in Russia's Disinformation and Propaganda Ecosystem," Global Engagement Center, January 2022, www.state.gov.

[46] *Council Regulation (EU) No 269/2014 of 17 March 2014 concerning restrictive measures in respect of actions undermining or threatening the territorial integrity, sovereignty and independence of Ukraine*, European Union, 17 March 2014, www.eur-lex.europa.eu.

[47] *COUNCIL REGULATION (EU) 2024/1745 of 24 June 2024 amending Regulation (EU) No 833/2014 concerning restrictive measures in view of Russia's actions destabilising the situation in Ukraine*, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L_202401745 (26.06.2024), p. 4.

[48] Ibidem.

[49] For more about maling influence of Voice of Europe see.: F. Bryjka, *Unravelling Russia's Network of Influence Agents in Europe*, „PISM Spotlight", No. 24, https://pism.pl/publications/unravelling-russias-network-of-influence-agents-in-europe (05.04.2024).

EU, but Western media have consistently reported that the EU has blocked access to websites of affected media outlets, and search engines and social media sites have also blocked access to sanctioned media organisations as part of EU broadcasting bans.

In practice, the EU imposes almost no costs on those using FIMI against Member States for their harmful effects. An example of this is the ability to view Russian websites (e.g., RT, or Sputnik) on EU territory, despite EU sanctions on these media imposed in March 2022. For example, RT has not stopped broadcasting in Germany despite the ban and even the punishment by the German media authority. On the other case, RT France tried to challenge the EU ban arguing that the Council had no power to impose such a ban and that it violated the EU Charter of Fundamental Rights, in particular the rights of the defence and the right to a fair hearing (Articles 41 and 48), the freedom to conduct a business (Article 16) and the freedom of expression (Article 11). On 30 March 2022, the President of the Court of Justice rejected RT France's application for an urgent preliminary ruling, and on 27 July, the Court, acting as a Grand Chamber, dismissed RT France's appeal in its entirety. In its judgment, the Court explicitly referred to the European Convention on Human Rights and Article 10 thereof, and indicated that Article 11 should be given equal weight, within the meaning of Article 52 of the Charter.35 The Court found that the restriction was proportionate and met the requirements of a restriction of fundamental rights in its entirety.[50] These examples proves that implementation of sanctions mainly depend on political willingness and legal systems of EU's member states.

After Russia's full-scale invasion of Ukraine, some countries (e.g., Czechia and Poland) briefly (for about 3-6 months) maintained blocks on websites spreading pro-Russian propaganda and disinformation, but national courts found insufficient legal grounds for such measures. In contrast, such measures were effectively taken by the Estonian authorities, where 53 TV channels and some 195 websites were blocked on the basis of a law prohibiting the promotion of an offensive war[51]. Between 2013–2021 Lithuania and Latvia also blocked access to Russian television channels ten and five times, respectively, predominantly sanctioning violations related to incitement to hatred or war[52]. The European Commission confirmed that Lithuania and Latvia correctly considered that television programmes calling for the agresssion and 'destruction' of various states constituted war propaganda, which justified the suspension of the broadcasts.[53] So, national efforts to curb disinformation depend on the will and determination of the government to actually counter it. Otherwise,

---

[50] J. Bayer, *The European response to Russian disinformation in the context of the war in Ukraine*, „Hungarian Journal of Legal Studies", 2023, 64 (4), p. 594.

[51] On 25 February 2022, the Estonian Consumer Protection and Technical Supervision Agency banned the rebroadcasting of five TV channels for broadcasting a speech by the President of the Russian Federation that justified military aggression and violated the Media Services Act. The agency continued to monitor and take action against channels and websites spreading harmful content. On 4 August 2022, it ordered the blocking of four websites promoting war propaganda, supporting crimes of aggression, and inciting hatred, thus threatening public order. Further measures were taken on 4 May 2023, when Estonia restricted access to 195 websites and 51 TV channels to protect its information space and enforce sanctions. Such actions have been regularly implemented, showcasing Estonia's ongoing commitment to safeguarding its information environment from disinformation.

[52] The domestic media authority based its decisions on Articles 3(4)(a)(i) and 6 of the AVMS Directive, which allow for the suspension of television programmes if they incite hatred on the basis of certain criteria, see: Sten Hansson et al., 'COVID-19 Information Disorder: Six Types of Harmful Information during the Pandemic in Europe', *Journal of Risk Research* 24, no. 3–4 (3 April 2021): 380–93, https://doi.org/10.1080/13669877.2020.1871058.

[53] J. Bayer, *The European response to Russian disinformation in the context of the war in Ukraine*, „Hungarian Journal of Legal Studies", 2023, 64 (4), p. 592.

disinformation actors are able to circumvent restrictions by using new servers and proxies that enable them to spread false and manipulated content.

5. Conclusions

So far, the EU's response to FIMI has focused on measures directed at strengthening societal resilience, reinforcing strategic communication, debunking, "naming and shaming", and imposing restrictive measures (international sanctions). Almost each tool in the FIMI Toolbox should be expanded upon and further developed.

The EU has significantly increased its situational awareness concerning threats stemming from foreign information manipulation and interference over the past decade. It has put forward a common analytical framework and developed a set of tools to counter the problem. However the existing regulatory framework and institutional capacities are still insufficient to effectively protect the information space from malign activity. The Digital Services Act, although ground breaking in many aspects will not in itself eradicate online information manipulation. Neither will digital, media and information literacy programs make our societies immune to all incidents of information manipulation. Foreign actors will continue to find ways to bypass sanctions and EU citizens will at times be persuaded to believe conspiracy theories. There is no one magic solution to the problem of disinformation. Nevertheless the level of harm to our cohesion and public security requires that all tools from the FIMI toolbox be expanded upon and implemented to their full extent by EU Member States. Further efforts in coordination, exchange of information and common action are also needed. To do that the EU must dedicate far more meaningful financial and human resources then it is currently doing and the EU Member States will need to demonstrate continuous political will in addressing the threat.

The ineffectiveness of the EU's response system to FIMI is the result of varying degrees of progress by individual EU countries in countering FIMI, different regulations at the national level, a lack of political will to be more proactive, restrictions related to the protection of freedom of expression, or the provisions of the GDPR. The implementation this year of the Digital Service Act (DSA), which is expected to increase the ability of states to influence online platforms to combat and remove illegal content, is expected to help change this.

The low level of standardisation of methods for detecting and analysing FIMI incidents hinders the exchange of information between Member States - both state administrations and NGOs. The lack of standardisation hinders the integration of the data held, which slows down the response to ongoing operations. In order for the defenders community to be able to effectively support their governments, as well as the EU, in terms of collective responses, there is a need to standardise FIMI analysis methods based on the ABCDE, DISARM, STIX framework.

Part II – STRATEGIES AND POLICIES

Filip Bryjka, Paweł Kasprzyk

In this section of the report, we will focus on analysing how EU Member States include countering FIMI and/or disinformation in their strategic documents and policy frameworks. We will discuss how they set out strategic objectives for countering FIMI or disinformation, whether these documents point to specific solutions for response, building institutional capacity, regulations and social resilience, or whether they merely characterise the problem. Attention of research focuses on countries that have adopted dedicated strategies, sectoral strategies (eg. cybersecurity strategies), national action plans and road maps focused on countering FIMI or disinformation.

2.1. Review of strategic documents

Strategies set the directions of a state's policy in specific areas of its functioning. The most important is the national security strategy. It is there that the role of the state resulting from its position and potential should be defined. The national security strategy also identifies the security environment in which the state operates. It identifies the national interests and strategic objectives of the state, which it seeks to realise (usually in a 5-10 year timeframe). National security strategies are therefore a kind of general determinant of the direction of the state's policy that facilitates the navigation and definition of specific sectoral objectives and the ways and concepts for their implementation. It is from this overarching document that directional strategies (e.g. cyber security, defence, military, foreign policy, education, migration, etc.) are derived. Instead of these, countries sometimes choose to adopt documents that formally have a lower profile (e.g. national action plans, road maps etc.) but allow for the setting of courses of action to be achieved in a shorter time frame (2-5 years).

The research shows that only three Member States have adopted or are advanced in the process of adopting startegies specifically dedicated to countering disinformation and FIMI. Nevertheless, a majority of EU states consider FIMI threats in their national security strategies (77,7%). Moreover, a significant share of EU Member States consider countering FIMI in their cybersecurity strategies (88%). These updates mainly occurred between 2017 and 2024 and had been significantly influenced by unfolding events, including the Russian hybrid aggression against Ukraine in 2014, increasing Russian interference in elections in the US and European countries (from 2016), disinformation campaings related to COVID-19 and war propaganda related to Russian full-scale invasion of Ukraine. Only a few Member States have thus far neither updated their national security strategies nor inscribed the threat of disinformation in any other strategic documents.

It should be noted that not all the Member States who have included mentions of FIMI and disinformation in their cybersecurity strategies have also addressed these threats in their national security strategies. In other words on the issue of countering FIMI and disinformation some, but not all Member States have decided to complement their national security strategies with cybersecurity strategies whilst some have adopted cybersecurity strategies without ever addressing the threat in a national security strategy. This is an important observation because cybersecurity strategies are documents that focus primarily on the technical issues of the problem, which occurs in the cyber domain. They identify disinformation campaigns, fake news, deepfakes, and the dissemination of disinformation in cyberspace as challenges. These are viewed as attempts to manipulate and polarize public opinion with the intention to alter perceptions of reality. For example, Germany's Cyber Security Strategy (2021) emphasises the need to protect media companies' websites from cyber-attacks. This approach indicates

that the German authorities identify cyberspace and, in particular, digital media as a major area of defence against disinformation. Thus, linking the countering of threats of this kind to cyber security. This may limit defence to technical activities related to the defence of information and communication infrastructure against activities identified as part of hostile operations[54].

	National strategy	**Dedicated strategy**	**Cybersecurity strategies**	**National action plans or road maps**	**Other relevant documents**
Austria	Austrian Security Strategy (2013) (no mentioning of disinformation)	-	Austrian Cybersecurity Strategy (2021)	Digital Action Plan for Austria: Goals, Guidelines and Principles (2020); Action Plan Deepfake (2022);	Digital Sovereignty for Austria (2023)
Belgium	National Security Strategy (2021)	-	Cybersecurity Strategy for 2021-2025	-	-
Bulgaria	National Security Strategy (2018)	-	National Cyber Security Strategy (2023)	-	Bulgaria-US Memorandum of Understanding on combating disinformation
Croatia	The Republic of Croatia National Security Strategy (2017) (no mentioning of disinformation but hybrid threats and radicalisation)	-	The National Cyber Security Strategy (2015) (no mentioning of disinformation)	-	-
Cyprus	-	-	Cyprus Cyber Security Strategy (2012) (no mentioning of disinformation)	-	-
Czech Republic	National Security Strategy 2023	National Strategy for Countering Hybrid Interference (2021)	Cybersecurity Strategy 2021-2025	Education Policy Strategy	National Defence Strategy (2023)
Denmark	Danish Security and Defence towards 2035	-	National Strategy for Cyber and Information	Action Plan to safeguard Danish democracy and society (2019)	National Digitalisation Strategy (2022)

[54] Bundesministerium des Innern, für Bau und Heimat, *Cybersicherheitsstrategie für Deutschland*, Bundesministerium des Innern 2021, https://www.bmi.bund.de/SharedDocs/downloads/DE/veroeffentlichungen/2021/09/cybersicherheitsstrategie-2021.html.

			Security (2022–2024)		
Estonia	National Security Policy (2017) National Security Concept of Estonia (2023)	-	Government Cyber Security Strategy (2019-2022) (no mentioning disinformation)	-	National Defence Development Plan 2031
Finland	Security Strategy for Society (2017) – to be renewed by end of 20224 In march 2024 work began on a national security strategy – publication planned by June 2025	-	Finland's Cyber Security Strategy 2019 Finland's Cyber Security Strategy 2024-2035(October 2024)	Countering disinformation – A guidebook for communicators on countering information influencing (2019) Media literacy and the national education strategy	Government's Defence Report (2021) Government report on changes in the security environment (2022) Government Programme (2023) Government Report on Finnish foreign and security policy (2024)
France	National Strategic Review (2022)	-	-	-	Report on information manipulation was published by the Policy Planning Staff (CAPS, Ministry for Europe and Foreign Affairs) and the Institute for Strategic Research (IRSEM, Ministry for the Armed Forces) [2018]; Enlightenment in the Digital Age Report (2022)
Germany	National Security Strategy 2023	-	Cyber Security Strategy (2021)	-	-
Greece	-	-	National Cyber Security Strategy (version 2.0)	-	-
Hungary	National Security Strategy (2021)	-	-	-	-

Ireland	-	In progress	National Cyber Security Strategy (2019–2024)	-	-
Italy	-	-	- National Cyber Security Strategy (2022-2026)	-	-
Latvia	National Security Concept (2023)	-	-The Cybersecurity Strategy (2023-2026)	Conceptual Report on the National Strategic Communication and Security of the Information Space 2023-2027	National Development Plan for 2021-2027
Lithuania	National Security Strategy (2021)	-	National Cyber Security Strategy (2018)	-	-
Luxembourg	Luxembourg Defence Guidelines 2035	-	National Cybersecurity Strategy IV(2021-2025)	-	-
Malta	-	-	National Cybersecurity Strategy (2023-2026)	-	Malta Information Technology Agency strategy for 2023-2026 Foreign Policy Strategy (2023)
The Netherlands	Security Strategy for the Kingdom of the Netherlands (2023-2029)	All-Government Strategy for Effectively Combating Disinformation (2022) Government-wide strategy for effectively tackling disinformation (2019)	Netherlands Cybersecurity Strategy (2022-2028)	Nationwide Response Framework against State-Sponsored Actors	-
Poland	National Security Strategy (2020)	Drafted Information Security Doctrine (2015) – not adopted	Cyber Security Strategy 2019-2024	-	-
Portugal	Strategic Concept of National Defence (no mentioning of disinformation)	-	National Cyberspace Security Strategy 2019-2023	-	-
Romania	National Public Order and Security	Drafted National Strategy for Strategic Communication	National Cyber Strategy for 2022-2027 (20217)	-	National Strategy in the field of Artificial

	Strategy 2023 – 2027 National Defence Strategy 2020-2024	and Combating Disinformation (2020) – not adopted			Intelligence 2024-2027 US-Romania Memorandum of Understanding to strengthen cooperation on countering FIMI
Slovakia	Security Strategy from (2021)	Concept for Combating Hybrid Threats (2018)	National Cyber Security Strategy (2021-2025)	Action Plan for Coordination against Hybrid Threats 2022-2024 Strategic Communication Concept of the Slovak Republic (2023)	-
Slovenia	National Security Strategy (2020)	-	-Cyber Security Strategy (2016) (no mentioning of disinformation)	-	-
Spain	National Security Strategy (2021)	-	Estrategia Nacional de Ciberseguridad (2019) (no mentioning of disinformation)	National Procedure Against Disinformation	-
Sweden	National Security Strategy (2024)	-	National Cyber Security Strategy (2016)	Countering Information Influence Activities: A Handbook for Communicators (2018) The Psychological Defence Agency's Handbook to recognise and deal with disinformation, misleading information, and propaganda (2023)	Total Defence 2021-2025 Government Bill 2024 The Swedish Defence Commission Report

Source: own study

2.2. EU Member State's strategies to counter disinformation and FIMI

Only two EU countries currently have a strategy dedicated to countering disinformation: Latvia[55] and the Netherlands.[56] In Ireland,[57] work on a similar strategy is well underway.

While several EU countries, especially in Central and Eastern Europe, address the threat of disinformation and FIMI, to a varying degree, in their national security strategies and/or other strategic documents, the Nordic countries can be seen to approach the problem in a systemic way, implementing a whole-of-government approach through a series of subsequent documents. Below is a brief summary of the existing or planned strategies dedicated to countering disinformation.

2.2.1. The Netherlands

Several Dutch strategic documents provide policy frameworks that contribute to the countering of disinformation and FIMI. Most notably these include: The Security Strategy for the Kingdom of the Netherlands (2023-2029),[58] the Netherlands Cybersecurity Strategy (2022-2028)[59] and the Nationwide Response Framework against State-Sponsored Actors.[60] Most importantly however, the Netherlands is the first country in the EU to have adopted a national strategy dedicated specifically to countering disinformation and FIMI.

The first *Government-wide strategy for effectively tackling disinformation* was announced by the Minister of the Interior and Kingdom Relations in October 2019. The strategy was constructed around three lines of action: prevention, strengthened messaging and, if necessary, response.[61] Over time however, the government came to realize that the dissemination of both disinformation and misinformation has in fact increased since then. Therefore, in December 2022, a new *All-Government Strategy for Effectively Combating*

---

[55] Cabinet of Ministers of the Republic of Latvia. *The National Concept on Strategic Communication and Security of the Information Space 2023–2027,* 1–23. https://www.mk.gov.lv/en/valsts-strategiskas-komunikacijas-un-informativas-telpas-drosibas-koncepcija?utm_source=https%3A%2F%2Fwww.google.com%2F [date published: 20.03.2023].

[56] Ministry of the Interior and Kingdom Relations (of the Netherlands). *Government-wide strategy for effectively tackling disinformation, 1*–18. https://www.government.nl/documents/parliamentary-documents/2022/12/23/government-wide-strategy-for-effectively-tackling-disinformation [date published: 23.12.2022].

[57] Department of Tourism, Culture, Arts, Gaeltacht, Sport and Media (of Ireland). *National Counter Disinformation Strategy Working Group.* https://www.gov.ie/en/publication/04f9e-national-counter-disinformation-strategy-working-group/ [date published: 30 March 2023].

[58] Government of the Netherlands. *Security Strategy for the Kingdom of the Netherlands.* [date published: 03.04.2023] https://www.government.nl/documents/publications/2023/04/03/security-strategy-for-the-kingdom-of-the-netherlands

[59] Ministry of Justice and Security of the Netherlands/National Cyber Security Centre. *The Netherlands Cybersecurity Strategy 2022-2028.* [date published 31.01.2023]. https://english.ncsc.nl/publications/publications/2022/december/06/the-netherlands-cybersecurity-strategy-2022-2028

[60] Government of the Netherlands. *Letter to Parliament on tackling state threats and presenting a threat assessment of state actors*. [date published: 28.11.2022] https://www.rijksoverheid.nl/documenten/kamerstukken/2022/11/28/tk-aanpak-statelijke-dreigingen-en-aanbieding-dreigingsbeeld-statelijke-actoren-2

[61] House of Representatives of the Netherlands. *Policy efforts to protect democracy against disinformation*. [date published: 18.10.2019]. https://www.tweedekamer.nl/kamerstukken/brieven_regering/detail?id=2019D41916&did=2019D41916

Disinformation was published. The new Dutch strategy highlights the importance of establishing a set of actions for countering disinformation.[62] In addition to the three lines of action listed in the previous strategy two more have been added in the new document: strengthening free and open public debate (including by means of maintaining a pluralistic media landscape and importance of investigative journalism), and reducing the impact of disinformation (including by raising awareness of disinformation among state institutions).

According to the Dutch *Government-wide strategy for effectively tackling disinformation*, the approach to addressing FIMI fits within the broader approach to address hybrid threats.[63] Nevertheless, multiple of the countermeasures envisaged to counter disinformation would likely also serve the purpose of countering FIMI since disinformation is often a key component of FIMI. Fully acknowledging that disinformation is not disseminated by state actors alone, the strategy nevertheless points to an increasingly assertive attitude and an increased use of information operations and disinformation to serve political interests by foreign state actors. Several references to FIMI as a specific point of concern are made as it is considered to pose a risk to national security, but also for the stability and security of international organizations that the Netherlands is part of, such as the EU and NATO.

The Dutch strategy underlines that the democratic rule of law, freedom of speech and freedom of the press must take center stage and that qualifying disinformation as such and fact-checking are not primary government duties.[64]

Recognizing that the public debate is increasingly conducted on large and internationally operating platforms and that it has become increasingly complicated to recognise disinformation, the strategy places strong emphasis on stimulating and using public alternatives to online platforms.[65]

The strategy places strong emphasis on the importance of implementing and enforcing a number of legislative frameworks at EU level, most notably the EU Digital Services Act (DSA), the European Media Freedom Act and the (voluntary) EU Code of Practice on Disinformation. It highlights the role of the government and the coordinated approach of state institutions and agencies to counter the threat but also recognises that as a global phenomenon, disinformation requires cooperation from a broad and diverse range of stakeholders and transnational networks. It therefore envisages a role for non-state actors, including civil society organizations, researchers, the academia, journalists, independent media and online platforms stakeholders in awareness raising efforts and other aspects of the strategies' implementation.

Finally, the Netherlands is committed to developing an effective response, where possible in collaboration with national and international partners (primarily within the EU context albeit also the OECD, NATO and the G7). The strategy dedicates considerable attention to the promotion of norms and values to internationally shared standards for tackling disinformation. The Netherlands advocates an alternative to content control that safeguards human rights and effectively counteracts disinformation campaigns."[66]

---

[62] Ministry of the Interior and Kingdom Relations (of the Netherlands). *Government-wide strategy for effectively tackling disinformation,* [date published: 23.12.2022]. https://www.government.nl/documents/parliamentary-documents/2022/12/23/government-wide-strategy-for-effectively-tackling-disinformation, p. 5.
[63] Ibidem, p. 10.
[64] Ibidem, p. 5.
[65] Ibidem, p. 6.
[66] Ibidem, p. 9, 12.

2.2.2. Latvia

Latvia treats countering FIMI as a part of its defence and deterrence capabilities[67]. The Latvian authorities have taken several actions to strengthen the security of the country and society. Since 2023, the National Security Concept has stated that a key threat comes from disinformation campaigns, the spread of misleading narratives, and exploring the potential for dissent and conflict in society[68]. In particular, the concept highlights Russian interference in Latvia's political processes. The document states that "the current legal regulation of media activities does not address the current challenges to the security of the Latvian information space". The Concept also includes a separate paragraph on conducting media policy discussions at the EU level (mostly instructions to social media companies to prevent the spread of false information, primarily through the European Democracy Action Plan). Furthermore, in relation to manipulation in the information space, the National Development Plan for 2021-2027 recommends strengthening national information space, preventing disinformation campaigns, and improving media literacy. The plan stresses, that "the content created in the information space, including the media, helps to sustain democracy and strengthen civic values. Access to high-quality media content in the national language and sufficient and high-quality information about what is happening in society also strengthens us as a society and a democratic country"[69].

The most important guidelines from the Latvian authorities regarding FIMI can be found in the "Conceptual Report on the National Strategic Communication and Security of the Information Space 2023-2027"[70]. This is a strategic medium-term policy planning document that sets out the national vision and objectives for strengthening information space security, including the development of strategic communication capabilities. The document defines six main lines of action to strengthen the security of the national information space and to put into practice models of coordination and cooperation: 1) implementation and development of national strategic communication capabilities, 2) measures to make the information space resilient to security threats, 3) strengthening and improving the media environment, 4) an engaged and resilient society, 5) partnership with organised civil society, the private and academic sectors, and 6) international cooperation[71]. The concept is complemented with an action plan, which is not publicly available. According to the concept report, it is expected that the implementation of solutions provided in the concept report will strengthen society's

---

[67] THE REGULATION OF FACT-CHECKING AND DISINFORMATION IN THE BALTIC STATES', *Becid* (blog), May 2024, https://becid.eu/results_and_studies/the-regulation-of-fact-checking-and-disinformation-in-the-baltic-states/

[68] Johannes Voltri, 'Countering Russian Information Influence in the Baltic States: A Comparison of Approaches Adopted in Estonia, Latvia, And Lithuania', 2022, p. 176, https://www.kvak.ee/files/2023/01/Sojateadlane-19-2022-Johannes-Voltri-COUNTERING-RUSSIAN-INFORMATION-INFLUENCE-IN-THE-BALTIC-STATES-A-COMPARISON-OF-APPROACHES-ADOPTED-IN-ESTONIA-LATVIA-AND-LITHUANIA.pdf.

[69] Par Latvijas Nacionālo attīstības plānu 2021.–2027. gadam (NAP2027), Latvijas Vēstnesis, 127, 06.07.2020, https://likumi.lv/ta/id/315879-par-latvijas-nacionalo-attistibas-planu-20212027-gadam-nap2027

[70] Par Valdības rīcības plānu Deklarācijas par Evikas Siliņas vadītā Ministru kabineta iecerēto darbību īstenošanai, Latvijas Vēstnesis, 16, 23 January 2024, https://likumi.lv/ta/id/349266-par-valdibas-ricibas-planu-deklaracijas-par-evikas-silinas-vadita-ministru-kabineta-iecereto-darbibu-istenosanai

[71] Par Valdības rīcības plānu Deklarācijas par Evikas Siliņas vadītā Ministru kabineta iecerēto darbību īstenošanai, Latvijas Vēstnesis, 16, 23 January 2024, https://likumi.lv/ta/id/349266-par-valdibas-ricibas-planu-deklaracijas-par-evikas-silinas-vadita-ministru-kabineta-iecereto-darbibu-istenosanai

sense of belonging to Latvia, Europe and its values, and citizens' support and trust in government policies and communication will gradually increase.

In Latvia's view, the best way to combat FIMI is through effective communication by state and local authorities with their target audiences, a strong and high-quality media environment and journalism, and a skilled, educated, and engaged public capable of recognizing and resisting manipulation of the information space. Strengthening each of these contributes to national security. Latvia takes a whole-of-society approach to cyber and information security, taking into account the weaponization of large data ecosystems, hard-to-analyse audio and visual content, problematic user behavior and evolving media consumption, as well as technological dependence on China. Latvia (like Lithuania) is an example of a blocking strategy, where the existence of an 'other' is recognised and dealt with. Instead of countering false information by projecting its versions of reality, the state protects its narratives by blocking those of an opponent.

2.2.3. Ireland

In 2020, the Irish Government established the Future of the Media Commission and tasked it with developing recommendations for sustainable public funding and other support to ensure the viability, independence and ability of the media in Ireland to meet public service objectives. The Commission's report, released in July 2022, contains a total of 50 recommendations that, in effect, constitute a strategic agenda for the transformation of the Irish media sector. One of them is the development of a national counter disinformation strategy to enhance the trust and protect the safety of Irish users of global content platforms.[72]

While the Irish strategy is not finalised, much information can be drawn from publicly available strategy Working Group reports, its terms of reference and citizen scoping paper. The multi-stakeholder working group began its work in February 2023. It operates in three subgroups whose purpose is to inform the development of the Irish strategy on: (1) existing countermeasures, (2) the emerging regulatory environment, and (3) supporting journalism and providing public interest information. The Working Group shared five guiding principles around which the Strategy could be developed[73]:

1) Counter disinformation and protect freedom of speech using a rights based approach
2) Counter disinformation by building resilience and trust - at individual and societal levels
3) Counter disinformation through increased cooperation, collaboration and coordination
4) Counter disinformation through corporate accountability and regulatory enforcement
5) Counter disinformation through evidence based countermeasures and interventions.

The Irish national strategy for countering disinformation objectives are focused to enact coordinated efforts with relevant government ministries and agencies to counter coordinated campaigns targeting Ireland, developing effective monitoring and building relationships between different national actors, including researchers and media platforms. The latter would also require supporting fact-checking and disinformation research and independent journalism in countering disinformation and new initiatives in media literacy.

---

[72] The Future of Media Commission *Report of the Future of Media Commission, p. 250* https://www.gov.ie/pdf/?file=https://assets.gov.ie/229731/2f2be30d-d987-40cd-9cfe-aaa885104bc1.pdf#page=null *[date published: 12.07.2022]*

[73] Department of Tourism, Culture, Arts, Gaeltacht, Sport and Media (of Ireland). *National Counter Disinformation Strategy Scoping Paper,* p. 10–12. https://www.gov.ie/pdf/?file=https://assets.gov.ie/286028/37ceb147-b155-4655-af17-df6189be7928.pdf#page=n

The Irish strategy planners have put a strong emphasis on conducting wide public consultations as part of the process. According to the scoping document which formed the basis of a written public consultation, disinformation is a problem "because it is designed to create doubt and disruption. It distorts the nature of public discourse, undermining trust in sources of reliable information and negatively impacting people's ability to make informed decisions based on accurate information."[74]

2.2.4 The Nordics

None of the Nordic EU Member States, Finland, Sweden or Denmark, have dedicated strategies for countering disinformation or FIMI. However, the three countries have recognized the threat to the functioning of the democratic societies and discuss disinformation and FIMI in multiple other strategies and policies.

The three countries emphasise a whole-of-government and whole-of-society approach in countering FIMI and disinformation and highlight the importance of the civil society in countering threats in the information space. The Danish Security and Defence towards 2035 sees disinformation as part of a hybrid toolbox aimed at spreading instability and sowing discord in national public discourse and in NATO and the EU.[75] The Strategy discusses resilience against these threats as part of 'societal security' which covers more policy areas than the classic (military) preparedness. Accordingly, societal security against hybrid threats is handled nationally through a whole-of-government approach but the term is not further defined.[76]

The 2024 National Security Strategy of Sweden recognized influence campaigns and disinformation as a threat to Swedish democracy. Disinformation and cyber threats are mentioned specifically as a hybrid tool, when discussing capacity-building against hybrid threats.[77] Accordingly, managing these threats requires improved situational awareness and decision-making capacity and improved collaboration between different sectors and decision-making levels in society.[78] A similar approach was adapted in the Total Defence 2021-2025 Government Bill in Sweden which in relation to threats in the information space discusses threats of disinformation to the democratic society within the framework of hybrid threats and vulnerabilities brought by social and technological development.[79]

Similarly, the Finnish Government's Defence Report of 2021 notes that Finland's defense increasingly requires preparedness against threats beyond conventional military activity. The report refers to these threats as 'broad-spectrum influencing' which includes cyber and information influencing.[80]

In addition, the 2024 Government Report on Finnish foreign and security policy notes security challenges that emerging technologies can pose. It specifically mentions how the

---

[74] Department of Tourism, Culture, Arts, Gaeltacht, Sport and Media (of Ireland). *National Counter Disinformation Strategy Scoping Paper,* 1–15. https://www.gov.ie/pdf/?file=https://assets.gov.ie/286028/37ceb147-b155-4655-af17-df6189be7928.pdf#page=n

[75] Danish Ministry of Defence. *Danish Security and Defence towards 2035.* [date published: September 2022] https://www.fmn.dk/globalassets/fmn/dokumenter/strategi/rsa/-regeringens_security-policy-report_uk_web-.pdf, p. 20

[76] Ibidem, p. 20, 71-74

[77] Government Offices of Sweden/Prime Minister's Office. *National Security Strategy.* [date published: July 2024]. https://www.government.se/globalassets/government/national-security-strategy.pdf, p. 6, 20, 27, 30,40.

[78] Ibidem, p. 30.

[79] Ibidem, p. 51-52.

[80] The Finnish Government/Valtioneuvosto. *Government's Defence Report/Valtioneuvoston puolustusselonteko.* [date published: 09.09.2021] http://urn.fi/URN:ISBN:978-952-383-820-8, p. 18, 23

development of AI renders cyber attacks, information influencing and disinformation increasingly targeted and more effective and the need to build a national knowledge-base in countering disinformation. Among other measures it proposes developing information defense, diplomacy and strategic communication "tool boxes" as well as developing national guidelines for targeted and coherent cyber attribution activities, taking into account key allies and partners.[81]

Denmark also notes the challenge of disinformation and information influencing campaigns in its tech diplomacy and digitalisation strategies. For example, the Ministry of Foreign Affairs of Denmark's Strategy for Tech Diplomacy Denmark's tech diplomacy recognizes that new technologies may risk undermining international peace and security through "personally targeted disinformation on social media generated by artificial intelligence or future quantum computers capable of breaking existing encryption."[82] The Strategy calls for international partnerships, regulation, and cyber-diplomatic efforts to counter threats in the cyberspace, including disinformation campaigns.[83] It also advocates for a stronger public-private cooperation (nationally and internationally) and for increased responsibility of tech companies in countering cyberattacks and the spread of misinformation and disinformation on digital platforms.[84]

The Finnish Security Strategy for Society from as early as 2017, which sets the Finnish comprehensive security concept underlying the Finnish whole-of-government and whole-of-society approach to preparedness. Disinformation or information influencing are discussed in connection to cognitive resilience. The Strategy highlights the importance of the media in upholding and creating societal resilience and underlines the importance of citizens' skills in critical media literacy and basic digital skills in countering disinformation. It also notes that enhancing a trustworthy journalism and media environment strengthens civil participation and aids in countering disinformation. Moreover, effective, trustworthy, well-timed and well-planned communications are important in trust-building.[85]

The Comprehensive Security Concept of Finland from 2018 underscores that the primary defense against information influencing is an educated and media literate citizen. Media literacy and media education are part of the guiding provisions of the Finnish nationwide education strategy and have historically been part of the education programs from early childhood education until highschool/vocational training and are considered a civic skill.[86]

The Swedish approach also emphasises the role of the civil society and media actors in countering disinformation and FIMI. Moreover, The Countering Information Influence Activities: A Handbook for Communicators[87] aims to increase public communicators'

---

[81] The Finnish Government/Valtioneuvosto. *Government Report on Finnish foreign and security policy/Ulko- ja turvallisuuspoliittinen selonteko.* [date published: 20.06.2024]. https://urn.fi/URN:ISBN:978-952-383-890-1, p. 18, 28.
[82] Ibidem, p. 12
[83] Ibidem, p. 17, 18, 21
[84] Ibidem, p. 8, 17
See also Denmark's Ministry of Finance. *Danmarks digitaliseringsstrategi Sammen om den digitale udvikling.* [date published: May 2022].
https://www.regeringen.dk/media/11324/danmarks-digitaliseringsstrategi-sammen-om-den-digitale-udvikling.pdf
[85] The Finnish Security Committee/Turvallisuuskomitea. *Security Strategy for Society/Yhteiskunnan turvallisuusstrategia - Valtioneuvoston periaatepäätös.* [date published: 02.11.2017]
https://turvallisuuskomitea.fi/wp-content/uploads/2018/02/YTS_2017_suomi.pdf, 14, 23, 32, 89.
[86] Finland's Security Committee/Turvallisuuskomitea. *The Finnish comprehensive security concept/Turvallinen Suomi - Tietoja Suomen kokonaisturvallisuudesta.* [date published: 04.10.2018]
https://turvallisuuskomitea.fi/turvallinen-suomi-2018-tietoa-suomen-kokonaisturvallisuudesta/, p. 8, 23, 125.
[87] Swedish Civil Contingencies Agency/Swedish Psychological Defence Agency. *Countering*

awareness and understanding of information influence campaigns and develop their ability to respond to them.

The more recent 2023 handbook by the Psychological Defence Agency aims to strengthen the Swedish population's ability to identify and resist foreign influence campaigns. It contains tips and tools for recognizing attempts of foreign powers to influence the Swedish population.[88] Sweden has also made recent adjustments to the school education system to enhance media literacy, including critical digital literacy and online safety education. These new initiatives included increased learning with digital texts, media and tools, strengthening skills in critically evaluating sources and understanding of the impact of digitalisation on the individual and society.[89]

Denmark has multiple other initiatives to increase the Youth's media literacy skills, cyber competencies and to promote online safety in the country through formal and informal education, like its Nordic counterparts.[90]

The three countries also recognize that they, the EU and NATO may increasingly become targets of such operations in the future. For example, Finland's 2022 Government report on changes in the security environment was conducted in response to Russia's full-scale invasion of Ukraine in February 2022 describes the new threats in the Finnish security environment, including hybrid and information influencing, and notes that Finland will "strengthen its security" in response as the country is preparing for the possibility of becoming a target of hybrid influence activities both in the short and long term. The 2023 Government Programme introduced planned measures to counter hybrid threats and strengthen cyber and information security mainly by investing in education in the field.

Finland revised its Cyber Security Strategy in 2024 in response to an evolving operating environment in accordance with the Government Programme, but the strategy as such reflects a less shallow link between the cyber and information domains compared to the two other Nordic countries.[91]

---

information influence activities - A handbook for journalists. [last accessed: 26.07.2024]. https://mpf.se/download/18.5ed1a83718d2a5fd639d524/1706648817558/countering-information-influence-activities-a-handbook-for-journalists.pdf

[88] The Psychological Defence Agency. *DON'T BE FOOLED -A handbook to help you recognise and deal with disinformation, misleading information, and propaganda.* [date published: 2023] https://www.bliintelurad.se/assets/uploads/2024/04/Handbok-Dont-be-fooled-2023-EN-TA_240417.pdf

[89] The European Commission. *Media literacy and safe use of new media - Sweden.* [last update: 28.11.2023]. https://national-policies.eacea.ec.europa.eu/youthwiki/chapters/sweden/68-media-literacy-and-safe-use-of-new-media

The Government Offices of Sweden. *Nationell digitaliseringsstrategi för skolväsende/National digitization strategy for schools.* [date published: 19.10.2017]. https://www.regeringen.se/contentassets/72ff9b9845854d6c8689017999228e53/nationell-digitaliseringsstrategi-for-skolvasendet.pdf

Andric, A. *Sweden – National Digitalisation Strategy for the School System 2023-2027.* The European Union Digital Skills & Jobs Platform. [date published: 24.07.2023] https://digital-skills-jobs.europa.eu/en/actions/national-initiatives/national-strategies/sweden-national-digitalisation-strategy-school-0

[90] European Commission. *Denmark: Education and Training Media literacy and safe use of new media.* [date published: 25.03.2024] https://national-policies.eacea.ec.europa.eu/youthwiki/chapters/denmark/68-media-literacy-and-safe-use-of-new-media

[91] Finland's Prime Minister's Office. *Finland's Cyber Security Strategy 2024–2035.* [date published: October 2024]. https://julkaisut.valtioneuvosto.fi/handle/10024/165893

The Danish National Strategy for Cyber and Information Security (2022–2024) notes that the security of the cyber and information domain are connected: "certain authoritarian states are actively trying to undermine the application of international law in cyberspace and increase control over the internet, while at the same time exploiting the global ICT infrastructure to conduct cyberattacks, influence campaigns and aggressive cyber espionage."[92] The Strategy highlights the importance of international cooperation and equipping citizens and businesses with the tools and skills to navigate the digital sphere safely.[93] It foresees a number of strategic initiatives, including digital literacy measures such as equipping children, young people and adults with skills in digital literacy and strengthening society's access to cyber and information security skills through higher education and the allocation of more funding for new initiatives in digital security.[94]

While largely focused on the cyber domain, the Swedish Defence Commission report underlines the importance of systematic work on information and cyber security.[95] It notes synergies between the cyber and information domains, especially in connection to Russia's way of waging cyber warfare and hybrid attacks in connection to the full-scale invasion of Ukraine, and the potential threat it poses to Sweden and its Allies.[96] The 2016 National Cyber Security Strategy also sees connection between threats in the cyber domain, disinformation and influence campaigns and highlights the importance of media and news agencies, training, and the role of international cooperation in counteracting the effects of disinformation and influence campaigns.[97]

2.2.5. Czechia and Slovakia.

The event that changed the Czech Republic's approach to countering hybrid threats from Russia was the identification in 2021 of the perpetrators of a subversion operation against an ammunition depot in Vrbětice carried out in 2014 by Russian military intelligence (GRU) officers[98]. In 2021 Czech Republic adopted the *National Strategy for Countering Hybrid Interference*, which defines objectives and determines instruments essential for the protection of vital, strategic and other interests of the Czech Republic against hostile hybrid interference. The development of this document was comissioned by the 2016 National Security Audit. The Strategy is based on systemic, holistic, comprehensive and whole-of-society approach to assure societal and institutional resilience. It complements the existing system of security policy documents by formulating a comprehensive nationwide policy to counter hybrid interference[99]. The need to counter disinformation is also mentioned in: 1) the Security

---

[92] Denmark's Agency for Digital Government. *Danish National Strategy for Cyber- and Information Security 2022–2024.* [date published: December 2021]. https://en.digst.dk/strategy/the-danish-national-strategy-for-cyber-and-information-security/strategic-objectives/p. 33

[93] Ibidem, p. 5

[94] Ibidem, p.5, 23-25.

[95] Ibidem, p. 16.

[96] Ibidem, p. 29.

[97] Government Offices of Sweden/The Ministry of Justice. *A national cyber security strategy* (2016/17:213). [last accessed 26.07.2024]. https://www.government.se/contentassets/d87287e088834d9e8c08f28d0b9dda5b/a-national-cyber-security-strategy-skr.-201617213, p. 7, 23-24, 26.

[98] M. Gniazdowski, M. Wasiuta, *Russian attacks in the Czech Republic: domestic context, implications, perspectives, Center for Eastern Studies*, 20.04.2021, https://www.osw.waw.pl/en/publikacje/analyses/2021-04-20/russian-attacks-czech-republic-domestic-context-implications (acess 19.06.2024)

[99] The Strategy was developed in accordance with the Public Strategy Development Methodology authorised by the Czech Government Resolution No. 71 dated 28 January 2019, see: National Strategy for Countering Hybrid

Strategy of the Czech Republic of 28 June 2023; 2) the Defence Strategy of the Czech Republic of 4 October 2023; 3) the Cybersecurity Strategy 2021-2025 which emphasises the importance of strategic communication; and 4) the Education Policy Strategy, which identifies enhancing media literacy as one of its priorities.

Hybrid threats have been first recognized as an increasing security challenge for Slovakia in the 2020 Government Manifesto as well as in the new Slovak Security Strategy from 2021. The latter is an update of the 2005 strategy and indicates that to counter disinformation *"[...] the Slovak Republic will focus on establishing coordinated national mechanism for increasing resilience to disinformation and information operations. The aim is to strengthen the structures and decision-making processes of early identification, evaluation and response to influential and disinformation effects, as well as the implementation of systemic measures. The Slovak Republic will support the development of critical thinking, especially young people, and will use the best practices and recommendations of international organizations, as well as competent non-governmental sector, in the fight against disinformation and propaganda.*"[100]. The Strategy also announces that in its strategic communication, it will focus on the active presentation of its foreign policy and security interests. It will develop public administration capacities and strengthen effective mechanisms for cooperation with competent non-governmental, academic and media sectors aimed at combating disinformation and propaganda and support strategic communication. It will support the development of civil society and cooperation with the nongovernmental sector by adopting interministerial and sector-specific systemic measures, including financial ones, which will enable the non-governmental sector to develop its programs and capacities.

Despite the change of government in autumn 2023, Slovakia maintained a coordination model for strategic communication created on the basis of the 2018 document 'Concept for Combating Hybrid Threats'. It assumes the cooperation of two institutions: The Situation Centre of the Slovak Republic RS SITCENT (national focal point for hybrid threats) established in the Office of the Security Council of Slovakia) and the National Analytical Security Centre NBAC (national cooperative centre for hybrid threats; established within the Slovak Information Service). In March 2022, Slovakia adopted the 'Action Plan for Coordination against Hybrid Threats 2022-2024' (APHH). The document, is based on the 2021 'Security Strategy of the Slovak Republic' and the 'Programme Declaration of the Government for 2021-2024'. The APHH is the Slovak government's response to changes in the international security environment - it was intended to complement and strengthen the coordinated mechanism for combating hybrid threats. In June 2023, the Slovak government adopted the Strategic Communication Concept of the Slovak Republic aimed at improving the communication of institutions with citizens and thus reducing the possibility of an information vacuum that 'creates preconditions for the spread of half-truths or mystifications'. Thus, the Slovak government has fulfilled the commitment contained in the APHH.

2.2.6. Poland and Romania.

In the face of increased Russian interference (since 2020 actively supported by Belarus), Polish state agencies and civil society organisations have scaled-up capabilities and countermeasures. However, a coordinated response at state level is hindered by the absence of clear guidelines and common situational awareness. Poland had drafted an Information

---

Interference, Prague 2021, p. 3, https://mocr.army.cz/assets/informacni-servis/zpravodajstvi/national-strategy---aj-final.pdf (access 19.06.2024).

[100] *Security Strategy of the Slovak Republik,* 2021, p. 19, https://www.mzv.sk/documents/30297/4638226/security-strategy-of-the-slovak-republic.pdf [02.09.2024].

Security Doctrine[101] already in 2015, but the document had not been approved and the country still lacks a dedicated strategy for countering FIMI and disinformation. However, these threats are acknowledged in other Polish national strategies. The 2020 *National Security Strategy of the Republic of Poland*[102] recognises the Russian Federation as a threat actor that undertakes "multi-faceted and comprehensive actions using non-military means (including: cyber-attacks, disinformation) to destabilise the structures of Western states and societies and to create divisions among Allies." It makes clear that the digital revolution "also creates room for disinformation and manipulation of information, which requires effective strategic communication activities."[103] The strategy calls for the building of capabilities to protect the information space, counteract disinformation and increase public awareness of threats related to the manipulation of information through education. However, possible threats in the information space were presented superficially and no concrete solutions in the fight against disinformation are indicated.[104] It is hoped that these shortcomings will be addressed in the next National Security Strategy of the Republic of Poland[105], which is currently being prepared.

The threats as well as risks associated with technological developments and new global challenges, were described in more detail in the *Cybersecurity Strategy of the Republic of Poland for 2019–2024*.[106] The Act also addresses threats related to disinformation and foreign influence in cyberspace by including measures to protect critical infrastructure and counter cyber attacks, which are often linked to disinformation campaigns.

In Romania a framework document dedicated to building capacity to counter FIMI – the *National Strategy for Strategic Communication and Combating Disinformation* was developed in 2020 but the document is not been implemented. According to experts involved in the strategy-making process the document correlates with the policies of both the EU and NATO and its premise is to strengthen social resilience and to protect and maintain a credible and transparent information environment in Romania. The strategy proposes an inter-institutional approach for generating a coherent public discourse in collaboration with relevant stakeholders. The document distinguishes between two paths of action: proactive, oriented towards promoting democratic values and state policy objectives through narratives and political action, and reactive, according to emerging threats. The document was never publicly published nor subjected to public debate or consultation with civil society[107]. According to the experts the Strategy is reportedly not usable, due to its incompatibility with existing Romanian legislation. Thus in reality, Romania does not have a national strategy for

---

[101] *Projekt Doktryny bezpieczeństwa informacyjnego RP*, Biuro Bezpieczeństwa Narodowego, 24 July 2015, https://www.bbn.gov.pl/ftp/dok/01/Projekt_Doktryny_Bezpieczenstwa_Informacyjnego_RP.pdf

[102] Biura Bezpieczeństwa Narodowego. *The National Security Strategy of the Republic of Poland*, 1–38. https://www.bbn.gov.pl/ftp/dokumenty/National_Security_Strategy_of_the_Republic_of_Poland_2020.pdf [date published: 12.05.2020], p. 6.

[103] Ibidem, p. 8.

[104] P. Berlińska-Wojtas. *Bezpieczeństwo informacyjne RP w dobie COVID-19.* Zeszyty Naukowe Zbliżenia Cywilizacyjne XVII (1)/2021, 33–50. https://dx.doi.org/10.21784/ZC.2021.003 [date published: 28.03.2021], p. 42.

[105] *Rekomendacje do Strategii Bezpieczeństwa Narodowego Rzeczpospolitej Polskiej*, Biuro Bezpieczeństwa Narodowego, [*Recommendations for the National Security Strategy of the Republic of Poland*, National Security Bureau], 4 lipca 2024 r., p. 34-35.

[106] Ministerstwo Cyfryzacji. *Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019-2024,* 1–25. https://www.gov.pl/web/cyfryzacja/strategia-cyberbezpieczenstwa-rzeczypospolitej-polskiej-na-lata-2019-2024 [date published: 30.12.2019].

[107] *Is Romania ready to combat disinformation and communicate effectively? Preparedness to identify and counter information manipulation and malign influence in the context of the war in Ukraine*, Global Focus 9.01.2023, p. 2.

strategic communication and countering disinformation. While there were some legislative initiatives, unfortunately, none of them came to fruition[108].

To address strategic vacuum, in July 2024 the Romanian Government approved the *National Strategy in the field of Artificial Intelligence 2024-2027*. The Strategy describes AI as dual-use technology, increasingly in use as part of hybrid warfare, cyber-attacks, disinformation and influence operations. It also supports research into the ethical applications of AI tools in addressing societal challenges including those related to disinformation[109].

2.2.7. France

In France there is no general strategic document on countering FIMI or disinformation. However, some recommendations, as well as elements of strategy and policy planning can be found in various documents (reports, doctrines, strategic reviews), published under the auspices of the President of the Republic, Senate, Ministry of the Armed Forces or Ministry of Europe and Foreign Affairs.

In 2018 a report on information manipulation was published by the Policy Planning Staff (CAPS, Ministry for Europe and Foreign Affairs) and the Institute for Strategic Research (IRSEM, Ministry for the Armed Forces)[110]. The report concluded with 50 recommendations directed at: 1) government, 2) civil society and 3) private actors. Recommendations for the government included: a) avoiding a purely top-down governmental response and opting for a horizontal collaborative approach, relying on civil society; b) setting-up a dedicated permanent structure within a wider institutional network; c) adopting legislative measures against fake news, reinforcing legislation which punishes online harassment, and considering to make registration compulsory for foreign media (US example); d) investing in international exchange; e) promoting media literacy in schools. Recommendations for civil society included: a) enhancing fact-checking and using AI and automated language processing; b) developing normative initiatives (rankings, indexes, labels); c) adopting an international charter of journalistic ethics, in a collaborative manner; d) inciting researchers to intervene in public debates. Finally, with regard to private actors: a) requiring platforms to contribute to the funding of quality journalism and independent research; b) demanding the establishment of a new contract with users that is founded on new digital rights.

In 2021 President Emmanuel Macron launched a commission *Les Lumières à l'ère numérique* (Enlightenment in the Digital Age), chaired by sociologist Gérard Bronner, that brought together 14 experts: historians, political scientists, lawyers, journalists, teachers, sociologists, civil society representatives, in order to measure and understand the dangers that digital technology poses to national cohesion and democracy. The commission issued a report (January 2022)[111] with 30 recommendations, notably on: 1) supporting and reinforcing scientific research on disinformation; 2) adapting the Open CTI platform for sharing data on disinformation between government, researchers, platforms, journalists; 3) creating an inter-ministerial digital governance mechanism and developing a digital security culture that includes information risk and involves all state actors; 4) creating a mechanism of crisis

[108] This data comes from an expert interview held on 11.09.2024.
[109] *Strategia națională în domeniul inteligenței artificiale 2024-2027*, 2024, p. 7, 85, 86, 88, 116.
[110] J.-B. Jeangène Vilmer, A. Escorcia, M. Guillaume, J. Herrera, Information Manipulation: A Challenge for Our Democracies, report by the Policy Planning Staff (CAPS) of the Ministry for Europe and Foreign Affairs and the Institute for Strategic Research (IRSEM) of the Ministry for the Armed Forces, Paris, August 2018.
[111] Elysee, Les Lumières à l'ère numérique (01.2022)
https://www.elysee.fr/admin/upload/default/0001/12/127ff0d2978ad3ebf10be0881ccf87573fc0ec11.pdf

management at the EU level to react to massive information operations; 5) creating a co-regulation regime between platforms, regulators and civil society within the DSA framework; 6) reviewing all education processes to systemically develop critical thinking.

In 2021 the Ministry of Armed Forces published some elements of the L2I doctrine: *La lutte informatique d'influence*[112]. L2I refers to military operations conducted in the information layer of cyberspace to detect, characterize and counter attacks, support StratCom, inform or deceive, independently or in combination with other operations. The Military Programming for 2019-2025 gives appropriate means to cyber defense, further prioritized in the Strategic Review.

The 2022 National Strategic Review upgraded influence to a 6th strategic function (next to knowledge/ appreciation/ anticipation; deterrence; protection/ resilience; prevention; intervention. This upgrade guarantees prioritization and funding. "The aggressiveness shown by our competitors reminds us that nothing can be taken for granted: in addition to our diplomatic, economic and strategic interests, the new battles for influence are about our ability to keep the French and European model alive, and to ensure that France's involvement on the international stage is understood and accepted. Inseparable from the other strategic functions described in this review, the influence function must be embodied in a national influence strategy that will set the general framework for action by all the actors concerned, determine the intentions and provide guidance for the national sectoral and/or geographical strategies. This strategy will aim to: defend France's long-term interests as well as universal values, the application of international law, multilateralism and the preservation of common goods; promote and showcase its commitments in all areas; respond or retaliate to manoeuvres or to attacks against our interests, particularly in the information field" [113].

2.3. Selected case studies of other EU Member States

In many EU Member States disinformation is treated as merely an element of hybrid threats (eg. **Belgium**[114]), cyber security or both (as in National Security Strategy of **Bulgaria**[115]). When using the term disinformation, some countries do not define it at all, some use the definition adopted by the EU in 2018 (e.g. **Latvia** and **Estonia**[116]), and many propose their own conceptual frameworks. Some of these were too general in nature, making it impossible to operationalise them. While it is noteworthy that **Lithuania** had been addressing disinformation long before EU countries recognised the problem, in the revised Public Information Act (2006) it was necessary to clarify the concept of disinformation defining it as „false information that is intentionally disseminated to the public"[117].

There are also purely academic blunders, such as first mentions of issues related to information manipulation in the **Spanish** *National Security Strategy* (2017) which specifically

---

[112] https://www.defense.gouv.fr/comcyber/nos-operations/lutte-informatique-dinfluence-l2i

[113] SGDSN, National Strategic Review 2022, p. 24.
https://www.sgdsn.gouv.fr/publications/revue-nationale-strategique-2022

[114] Comité stratégique du renseignement et de la sécurité, Stratégie de sécurité nationale, 1 Dec. 2021, p. 19, https://www.egmontinstitute.be/app/uploads/2022/02/NVS_Numerique_FR.pdf [09.06.2024]

[115] *Aktualizirana strategiâ za nacionalna sigurnost na Republika B"lgariâ*, 23.03.2018,
https://www.me.government.bg/files/useruploads/files/akt.strategiq2020.pdf, [Access: 20.07.2024].

[116] 'DEFENDING THE VOTE: ESTONIA CREATES A NETWORK TO COMBAT DISINFORMATION, 2016–2020', Global Challenges Election Disinformation, n.d.,
https://successfulsocieties.princeton.edu/sites/g/files/toruqf5601/files/TM_Estonia_Election_FINAL%20edited_JG.pdf.

[117] 'X-752 Lietuvos Respublikos Visuomenės Informavimo Įstatymo Pakeitimo Įstatymas', 11 July 2006, https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.280580.

listed "misinformation campaigns" as a threat instead of „disinformation campaigns", although the term misinformation refers to the unintentional dissemination of false or manipulated information (as opposed to deliberate disinformation).[118] However, this inconsistency has already been addressed in the Spanish *National Security Strategy* from 2021, where disinformation was described as one of the main threats for state security.

Germany's *Cyber Security Strategy* (2021) defines disinformation as "the deliberate dissemination of false or misleading information"[119]. The strategy highlights the particular threat posed by the dissemination of disinformation through online platforms that have been victims of cyber-attacks. The document indicates that disinformation activities may be part of broader hybrid operations conducted by foreign states.

In the case of **Hungary's** *National Security Strategy* the word "disinformation" appears only once (in chapter 5, paragraph 68). It is worth to underline that, the document's emphasis is not on the external sources of disinformation in Europe, but on "turning international public opinion against Hungary in an organised and systematic manner". Disinformation is therefore not seen as a threat to state security, but rather, as the authors themselves articulated, as an "attempt to restrict Hungary's ability to act"[120]. Given that this is the only strategic document of Hungary in which the concept of disinformation appears, and that its interpretation is at odds with approaches of all other EU countries, it can be concluded that in the case of Hungary the issue of information manipulation is not seen as a security threat at all.

As part of the implementation of the National Cyber Security Strategy 2022-2026, **Italy** plans to implement a national coordination action, consistent with initiatives adopted at EU level and in synergy with "like-minded countries", to prevent and combat online disinformation[121]. This action is to use the characteristics of the cyber domain to counter attempts to influence the country's political, economic and social processes[122].

2.4. Conclusions

Existing strategy documents do not use the term FIMI but disinformation, which is primarily due to the relatively recent (2023) development of the FIMI Framework. The lack of terminological standardisation leads to conceptual confusion, giving rise to possibility of different interpretations and, consequently, adapting different approaches and instruments in countering the problem.

---

[118] The document points out that "misinformation campaigns are not an isolated incident but in fact form part of a planned strategy: the so-called hybrid war, which combines everything from conventional forces to economic pressure and cyberattacks, see.: M. Gonzales, *Spain's national security strategy to include risk of disinformation campaigns*, El Pais, December 1, 2017, https://english.elpais.com/elpais/2017/12/01/inenglish/1512122156_659936.html

[119] Bundesministerium des Innern, für Bau und Heimat, *Cybersicherheitsstrategie für Deutschland*, Bundesministerium des Innern 2021, https://www.bmi.bund.de/SharedDocs/downloads/DE/veroeffentlichungen/2021/09/cybersicherheitsstrategie-2021.html.

[120] *Hungary's National Security Strategy*, 2021, https://honvedelem.hu/hirek/government-resolution-1163-2020-21st-april.html [Access: 30.07.2024]; C. Veress, *The Comparison Between the Hungarian and Romanian National Security Strategies*, „European Scientific Journal, ESJ", 2022/39, p. 133, 135–139.

[121] Agenzia per la Cybersicurezza Nazionale, *National Cybersecurity Strategy 2022 – 2026: Implementation Plan*, Presidenza del Consiglio dei Ministri 2022, 9, https://www.acn.gov.it/portale/en/strategia-nazionale-di-cybersicurezza, [accessed: 27.06.2024].

[122] Agenzia per la Cybersicurezza Nazionale, *National Cybersecurity Strategy 2022 – 2026: Implementation Plan*, Presidenza del Consiglio dei Ministri 2022, 9, https://www.acn.gov.it/portale/en/strategia-nazionale-di-cybersicurezza, [accessed: 27.06.2024].

Most of the EU member states' strategies, do not directly translate into comparable resilience against disinformation. Rather, it seems that in each of these countries, disinformation poses a problem, but in different ways, which, it can be argued, is greatly influenced by the factors specific to each national context. Countries approach disinformation differently. Elections, along with related disinformation content, are to a large extent influenced by national political, economic, and sociocultural specificities. Some forms of disinformation seem to be global, each country exhibits specific structural factors, strengths and weaknesses of the media system, practices of media use, and levels of trust in media, which together play a key role in how disinformation is received, perceived and used.

In the coming years EU Member States will face new challenges related to the threat of FIMI and disinformation. These challenges will be driven by technological advencements as well as increased geopolitical rivalries.

To effectively protect the information space for open, democratic debate, free of foreign interference and manipulation, EU Member States will need to dedicate significantly more attention and resources to countering the threat. The EU should assist Member States in standardisation efforts and promote best practices, including on coordination with non governmental organisations, media and the private sector as well as on maintaining institutional memory and on collective response measures.

Part III – INSTITUTIONAL CAPACITY

Agnieszka Cianciara, Kamila Szymańska

3.1. Institutionalization of coordination systems in the European Union member states

This subchapter seeks to map the processes and stages of institutionalization of coordination systems aimed at countering FIMI in the member states of the European Union.

The analysis is based on three key variables, related to: a) **centralized versus decentralized** nature of the coordination system; b) **government versus ministerial** level of coordination; c) existence of a **specialized agency** dedicated to countering FIMI.

Constellations of these variables allow to assign member states to three broad categories of: 1) **Champions** (high level of institutionalization); 2) **Aspiring Players** (medium level of institutionalization); 3) **Laggards** (low level of institutionalization).

States with high level of institutionalization (champions) feature a well-developed centralized coordination system, with a viable government level coordination mechanism and a specialized agency being established. This group is so far represented by only two member states: France and Sweden.

On the other side of the spectrum, states with low level of institutionalization (laggards) feature a very rudimentary, if any, coordination mechanism, which is typically, albeit not exclusively, characterized by ministry-level coordination, with no specialized agency being established. Examples of low level of institutionalization feature small member states and/ or states with relatively limited administrative capacities, including: Bulgaria, Cyprus, Hungary, Luxembourg, Malta, Romania. Relatively low level of institutionalization was also observed in Belgium, Denmark and Portugal.

States with medium level of institutionalization (aspiring players) feature diverse institutional solutions. The may have either centralized or decentralized coordination systems, with either government or ministerial level coordination mechanism. Their coordination systems are already fairly well developed and some of them experiment with specialized-agency-type solutions. Examples of medium level of institutionalization feature big member states, including Germany, Italy, Poland and Spain, as well as Netherlands and "eastern flank" states that take Russian threat actors seriously, especially Czechia, Estonia, Finland and Lithuania.

It should be noted that this analysis is based on data available in the public domain as well as subjective perceptions of experts who responded to the survey and participated in the interviews. It should further be noted that, due to security concerns and political sensitivities related to the fight against FIMI, not all coordination practices within the member states governments are likely to be disclosed in public.

3.1.1. Centralized versus decentralized nature of the coordination system

The vast majority of the EU member states have opted for decentralized coordination systems, whereas only a few have opted for centralized systems. A decentralized coordination system means that responsibilities in the field of countering FIMI are placed within various levels of government (central, regional, local), as well as with non-governmental stakeholders. A centralized coordination system means that responsibilities are predominantly, although not exclusively, placed within a central structure that features government-level coordination

mechanism and a specialized agency or an administrative unit dedicated to monitoring, analyzing and responding to FIMI.

Centralized coordination systems were identified in Czechia, France and Sweden.

Decentralized coordination systems with government-level coordination mechanism were identified notably in Estonia, Finland and Lithuania.

Decentralized coordination systems with ministry-level coordination mechanism were identified notably in Denmark, Germany, Netherlands and Poland.

Rudimentary institutional solutions, which are difficult to assign to any coordination typology at this stage of development, were identified notably in Bulgaria, Cyprus, Hungary, Luxembourg, Portugal and Romania. These countries do not have proper coordination systems in place, although there are institutions, and sometimes quite a significant number of them (Romania), that have formal responsibilities in the field of fighting disinformation. Typically, a leading, but not necessarily coordinative role in the field of strategic communication and countering disinformation is placed within Ministers of Foreign Affairs (Bulgaria, Portugal), albeit other solutions, including Ministry of Justice (Luxembourg) or Ministry of Interior (Cyprus) are also in place.

In some countries, such as Belgium, it is difficult to identify any type of a comprehensive institutional system of coordination, but rather "there are various dispersed initiatives that are not coordinated by state institutions", according to survey responders. Belgium is a peculiar case of a state with weak federal institutions, that is deeply divided along regional and linguistic lines. Local communities' information ecosystems are very connected to neighbour countries: France for Wallonia, and Netherlands for Flanders. Public space fragmentation around linguistic communities prevents strong national initiatives from emerging[123].

3.1.2. Government versus ministerial level of coordination

Only a minority of the EU member states have opted for a coordination mechanism placed at the central government level (under the authority of the head of government and/ or within his/ her office). This is notably the case of France or Sweden (within centralized coordination systems), but also Finland or Lithuania (within decentralized coordination systems).

In France, the Secretariat-General for Defense and National Security - under the direct authority of the Prime Minister - is responsible for countering FIMI at policy and operational level. This structure also provides the secretariat for the National Defense and Security Council, chaired by the President of the Republic, which is the leading body for defining France's security and defense policy. Placed at the heart of the executive, the Secretariat-General is in charge of inter-ministerial coordination regarding FIMI. It has three main missions: 1) crisis monitoring and alerting to threats and risks; 2) advising and drafting executive decisions regarding defense and national security; 3) operations, notably in the field of vigilance and protection against foreign digital interference service (via its technical service VIGINUM).

In Sweden it is the Prime Minister's Office that coordinates on national security issues. The Crisis Management Coordination Secretariat – under the National Security Adviser – is responsible for monitoring FIMI and bears overarching responsibility for FIMI-related issues within the Swedish Government Offices. In addition, the Ministry for Foreign Affairs is responsible for countering foreign malign information influence activities within the

[123] A. Alaphilippe, *Disinformation Landscape in Belgium*, EU DisinfoLab May 2023, https://www.disinfo.eu/wp-content/uploads/2023/05/20230509_BE_DisinfoFS.pdf [06.06.2024].

framework of foreign and security policy. The MFA has a coordinating role regarding strategic communication aimed at preventing and combating malign information influence and disinformation about Sweden abroad. Finally, the Ministry of Defense bears responsibility for the psychological defense and oversees the Swedish Psychological Defense Agency.

In contrast, Finland's comprehensive security model integrates a decentralized whole-of-government and whole-of-society approaches, involving authorities, business, NGOs, and citizens. Government-level coordination is overseen by the Prime Minister's Office, whereas the Government Situation Centre (VNTIKE), especially the Hybrid Team, manages a whole-of-government hybrid threat assessment cycle. The Preparedness Unit, and the Government's Operational Centre, established during Covid-19, manage preparedness coordination.[124]

In Lithuania, coordination at government level is ensured by the National Crisis Management Center, which operates at the level of the Lithuanian Government Office and was established in January 2023.[125] It employs approximately thirty experts and coordinates the work of ten institutions with regard to responding to FIMI, according to the survey. However, each state institution is responsible for monitoring information space within their own area of competence, and assessing incidents based on a pre-defined set of criteria and, if needed, reporting to the Centre that coordinates further communication. The Head of the Centre is government's vice-chancellor with direct access to the prime minister and involvement in coordination and operations on the one hand, but also strategic decision-making on the other.

Yet the vast majority of EU member states have opted for placing the coordination mechanism at the ministerial level. Ministries responsible for coordinating policies aimed at countering FIMI vary and it is difficult to detect any dominant pattern of convergence at this stage of institutionalization processes.

In some member states the leading institution seems to be the Ministry of Foreign Affairs. This is notably the case of Poland, where in May 2024 Plenipotentiary for Countering International Disinformation was appointed[126]. The Plenipotentiary is supported by the Department for Strategic Communications and Countering Foreign Disinformation of the MFA. However, responsibilities related to countering FIMI are also placed within the Chancellery of the Prime Minister, National Security Bureau, Ministry of Defence, Cyberspace Defence Forces, Government Security Centre, Ministry of Digital Affairs and various intelligence agencies. Interestingly, Poland had a brief episode (2022-2023) of a government level coordination mechanism managed by the Government Plenipotentiary for Security of Information Space[127]. However, his office was dissolved after the change of government in October 2023 due to heavy politicisation. It was admittedly involved in

---

[124] Fjäder, C. & Schalin, J. Building resilience to hybrid threats: Best practices in the Nordics. The European Centre of Excellence for Countering Hybrid Threats (HybridCoE). [date published: May 2024] https://www.hybridcoe.fi/wp-content/uploads/2024/05/20240527-Hybrid-CoE-Working-Paper-31-Building-resilience-to-hybrid-threats-WEB.pdf

[125] Seimas pritarė naujam krizių valdymo ir civilinės saugos modeliui, 8 December 2022, https://lrv.lt/lt/naujienos/seimas-pritare-naujam-kriziu-valdymo-ir-civilines-saugos-modeliui/?fbclid=IwAR3Ks1Idn6VDLM5UYzviZ2TQiVLbs8DvKPNAALAn2IGmrDReyzngGRdygs

[126] *Tomasz Chłoń pełnomocnikiem Ministra spraw zagranicznych ds. przeciwdziałania dezinformacji międzynarodowej*, https://www.gov.pl/web/dyplomacja/tomasz-chlon-pelnomocnikiem-ministra-spraw-zagranicznych-ds-przeciwdzialania-dezinformacji-miedzynarodowej, [14.05.2024].

[127] *Premier powołał Pełnomocnika Rządu ds. Bezpieczeństwa Przestrzeni Informacyjnej RP*, https://www.gov.pl/web/sluzby-specjalne/premier-powolal-pelnomocnika-rzadu-ds-bezpieczenstwa-przestrzeni-informacyjnej-rp [09.09.2022].

political campaigning aimed at discrediting the opposition as agents of (internal) disinformation.

In Germany, the Strategic Communications Plenipotentiary at the Ministry of Foreign Affairs is responsible for combating disinformation at the federal level. An important role is also played by the Inter-Ministerial Working Group on Hybrid Threats (AG Hybrid), Federal Office for the Protection of the Constitution and the Operational Communications Centre under the Bundeswehr's Cyber and Information Space Command. Yet, despite a number of sectoral institutions and cross-sectoral initiatives, the lack of central coordination between task forces and departments at ministerial level remains a problem, according to survey respondents.

In the Netherlands, the responsibility for coordinating the policy against disinformation is with the Minister of Interior and Kingdom Relations, but each ministry should respond effectively and appropriately when it faces disinformation affecting its own policy area[128]. Meanwhile in Denmark, coordination is spread across several ministries, with key responsibilities being placed with the Ministry of Defense and Ministry of Justice[129].

3.1.3. Existence of a specialized agency dedicated to countering FIMI

France and Sweden are the two EU member states that have already established and made fully operational specialized agencies dedicated exclusively to monitoring, analyzing and responding to FIMI.

VIGINUM (fr. *Service de **vigi**lance et protection contre les ingérences **num**ériques étrangères*; eng. Vigilance And Protection Service Against Foreign Digital Interference) is a technical and operation service created in 2021 and attached to the Secretariat-General for Defense and National Security under the authority of the Prime Minister. VIGINUM is a central part of the French coordination system, in charge of inter-ministerial coordination at the technical level. This inter-ministerial ecosystem features officials from VIGINUM, Operational Committee to Combat Information Manipulation (COLMI), Ministry of Europe and Foreign Affairs (MEAE), Ministry of Armed Forces and Ministry of Interior[130]. At the technical level, the VDC-P network (*Veille, Détection, Caractérisation et Proposition*/ Monitoring, Detection, Characterization and Proposal) brings together – under VIGINUM – different administrations with technical capabilities in the fight against information manipulation[131]. As of 2024 VIGINUM employs ca. 70 people, most of them in Operations

---

[128] Ministry of the Interior and Kingdom Relations (of the Netherlands). Government-wide strategy for effectively tackling disinformation, [date published: 23.12.2022].
https://www.government.nl/documents/parliamentary-documents/2022/12/23/government-wide-strategy-for-effectively-tackling-disinformation

[129] Fjäder, C. & Schalin, J. *Building resilience to hybrid threats: Best practices in the Nordics.* The European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE). [date published: May 2024]
https://www.hybridcoe.fi/wp-content/uploads/2024/05/20240527-Hybrid-CoE-Working-Paper-31-Building-resilience-to-hybrid-threats-WEB.pdf , p. 13.

[130] Charles Thépaut, Deputy Director of Monitoring and Strategy at the Ministry of Europe and Foreign Affairs, Twitter, 12.02.2024, https://x.com/diplocharlie/status/1757158603897626942 [05.06.2024].

[131] ASSEMBLÉE NATIONALE, SÉNAT : RAPPORT PUBLIC FAIT AU NOM DE LA DÉLÉGATION PARLEMENTAIRE AU RENSEIGNEMENT relatif à l'activité de la délégation parlementaire au renseignement pour l'année 2022-2023, 29.06.2023, p. 48 https://www.assemblee-nationale.fr/dyn/16/dossiers/activite_dpr_2022_2023 [05.06.2024]..

unit: OSINT analysts, geopolitical analysts and data lab analysts[132]. The agency has grown from 8 people in July 2021.[133]

The Swedish Psychological Defense Agency was established in the year 2022 and is answerable to the Ministry of Defense. The Agency leads the coordination and development of Sweden's psychological defense in collaboration with public authorities and other stakeholders. Similarly to French VIGINUM, it monitors external campaigns, whereas democratic principles forbid the agency to monitor domestic actors.[134] The Agency was established to identify, analyze and provide support in countering malign information influence and conduct work on preventing, detecting and counteracting information influence operations. It also aims at strengthening the citizens' ability to detect and resist malign influence campaigns and disinformation. This is achieved by cooperation with educating agencies, municipalities, regions and civil society organizations[135].

There are also recent developments in other EU member states that point to a nascent process of diffusion of the specialized agency solution. For instance, in June 2024 the German Federal Government created Central Office for the Recognition of Foreign Information Manipulation (*Zentralen Stelle zur Erkennung ausländischer Informationsmanipulation*)[136]. Its tasks are to identify the methods used by foreign influence campaigns, how to detect them at an early stage and to improve the federal government's ability to respond to such threats. The office reports to the Ministry of the Interior and is to cooperate with the Chancellor's Office, the Ministry of Foreign Affairs, the Ministry of Justice, and the Federal Press Office[137]. Currently, the number of staff is 10, with a target of 20.

Another example is Center on Information Resilience founded in 2022 as a pilot project by the Finnish National Emergence Supply Agency[138]. The aim was to develop policies and tools to combat malicious information influence operations, while acting as a national expertise hub for authorities, business and citizens. The Centre was founded after a preliminary study on information security by the National Emergence Supply Agency revealed significant national deficiencies in information security[139].

3.2. Use of digital and analytical tools by state institutions

---

[132] Interview by Agnieszka Cianciara: Laura Brincourt, Deputy Head of Coordination and Strategy Unit, VIGINUM/ SGDSN, Paris 26 April 2024.

[133] Alexis Bernigaud, Defending the Vote: France Acts to Combat Foreign Disinformation, 2021 – 2022, Innovations for Successful Societies, Trustees of Princeton University, 2023, https://successfulsocieties.princeton.edu/publications/defending-vote-france-acts-combat-foreign-disinformation-2021-%E2%80%93-2022 [05.06.2024].

[134] Giandomenico, J. & Linderstål, H. *Disinformation Landscape in Sweden.* [date published: May 2023]. https://www.disinfo.eu/wp-content/uploads/2023/05/Sweden_DisinfoFactsheet.pdf, p. 7-8.

[135] Psychological Defense Agency. *Our Mission.* [date published: 15.03.2024] https://mpf.se/psychological-defence-agency/about-us/our-mission

[136] https://www.bundestag.de/ausschuesse/a23_digitales/Anhoerungen/1022350-1022350

[137] https://www.deutschlandfunk.de/stelle-gegen-auslaendische-desinformation-inimmt-arbeit-auf-100.html

[138] Finnish National Emergency Supply Agency/Huoltovarmuuskeskus. *Finnish National Emergency Supply Agency builds capabilities to counter information influencing/ Huoltovarmuuskeskus rakentaa kykyä torjua informaatiovaikuttamista.* [date published: 17.08.2022] https://www.huoltovarmuuskeskus.fi/a/huoltovarmuuskeskus-rakentaa-kykya-torjua-informaatiovaikuttamista#

[139] Finnish National Emergency Supply Agency/Huoltovarmuuskeskus. *Countering information influencing - Preliminary report/Informaatiovaikuttamisen torjunta - Esiselvitys.* [date published: 01.12.2021]. https://www.huoltovarmuuskeskus.fi/files/d601de13993e8873d2d66bf379c35f13309dc42a/hvk-informaatiovaikuttamisen-torjunta-esiselvitys.pdf

This subchapter seeks to map the use of analytical frameworks, such as DISARM, and digital tools, such as Open CTI, to analyze FIMI across the EU member states. It should be noted that this exercise is based on data available in the public domain as well as information procured from experts who responded to the survey and participated in the interviews. It should further be noted that, due to security concerns and political sensitivities related to the fight against FIMI, operational and technical details of FIMI identification, analysis and response across the member states' administrations are not necessarily likely to be disclosed in public.

An overall conclusion emerging from the survey is that respondents affiliated with member states' public administrations are knowledgeable about tools used by state institutions, whereas those representing NGOs are knowledgeable about tools used by NGOs, but not state institutions. Respondents affiliated with academia or think-tanks usually possessed little knowledge with regard to tools used by both state institutions and NGOs. As a result, our respondents from member states such as Greece, Slovakia, Latvia, Czechia, or Finland were not able to tell us whether state institutions in their countries use any analytical or digital tools to analyze FIMI. In contrast, respondents from Italy, Malta and Portugal clearly declared that such tools are not used by state institutions in their countries.

It should be deduced from the above that knowledge about the usage of tools by governmental or non-governmental actors is very scattered and fragmented even in the case of experts who declare high level of knowledge and some years of experience in the disinformation/ FIMI field in their country. A good illustration of this problem is provided by survey respondents from Poland. Whereas some of the Polish academia/ think-tank experts did not know whether such tools are used at all, others pointed out that NGOs use ABCDE framework, while a respondent from the public administration declared that state institutions indeed use DISARM, STIX and Open CTI tools.

As a result, there is a clear need for more comprehensive knowledge sharing and cooperation across sectors and member states.

Below, examples of usages of analytical and digital tools are outlined where there is clear evidence that such tools are used by state institutions responsible for identifying, analyzing and responding to FIMI.

The French agency VIGINUM is quite open and transparent with regard to their working methods related to identification and analysis of FIMI. In January 2024 VIGINUM published a doctrine (Version 1.0) related to usage of STIX (Structured Thread Information Expression) 2.1 and OpenCTI tools[140], which means that the agency is at the relatively early stage of using this toolbox. DISARM analytical framework, on the other hand, has been used by VIGINUM analysts on a regular basis. It is worth underlining that VIGINUM has a legal mandate[141] that rigorously defines what exactly they can detect and characterize and the scope and type of data they can collect. As to the former, they only analyze information operations executed by

[140] VIGINUM : Capitalisation des campagnes et incidents de manipulation de l'information dans OpenCTI. Doctrine d'utilisation de VIGINUM. Version 1.0 | janvier 2024, https://github.com/VIGINUM-FR/Doctrine-OpenCTI/blob/main/SGDSN_VIGINUM_DoctrineOpenCTI.pdf [05.06.2024].

[141] Décret n° 2021-922 du 13 juillet 2021 portant création, auprès du secrétaire général de la défense et de la sécurité nationale, d'un service à compétence nationale dénommé « service de vigilance et de protection contre les ingérences numériques étrangères, https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000043788361; Décret n° 2021-1587 du 7 décembre 2021 portant autorisation d'un traitement automatisé de données à caractère personnel dans le but d'identifier les ingérences numériques étrangères, https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000044454057.

a foreign state or foreign non-state actor; that involve massive, purposeful, artificial or automated distribution; that feature manifestly inaccurate or misleading content; and constitute an attack on the fundamental interests of the state. They only use open source. Each time they need authorization for automated data collection for a maximum of 6 months, and then after 4 months from the start of the collection the rough data must be deleted. The mandate is so strict that the Scientific and Ethical Council that oversees VIGINUM suggested in its 2023 annual public report that the mandate should be extended, so that they can also monitor smaller platforms of less than 5 million users[142].

In Lithuania, both state institutions and non-governmental organizations are using ABCDE, DISARM, Open CTI and STIX tools, according to survey respondents. The National Crisis Management Center within the Lithuanian Government Office first used Open CTI as a pilot project before the NATO summit that took place in Vilnius in July 2023[143].

Similarly in Ireland, both state institutions and non-governmental organizations use DISARM, Open CTI and STIX tools. In addition, survey respondents from the business sector reported the use of MITRE ATT&CK. This is a "knowledge base used as a foundation for the development of specific threat models and methodologies in the private sector, in government, and in the cybersecurity product and service community"[144].

Dutch state institutions are solely using the DISARM analytical tool, according to survey respondents from the public administration sector. It was confirmed that ABCDE and DISARM frameworks are also used by non-governmental organizations in Germany. However, according to a German respondent from the military sector usage of digital tools and analytical frameworks by state institutions to identify and analyze FIMI constitutes classified information.

In some EU member states, such as Belgium or Bulgaria, the use of analytical and digital tools seems to be more widespread among the non-governmental organizations than state institutions. In particular, Bulgarian NGOs provide trainings to public administration staff as to how to use DISARM, Open CTI and STIX . In addition, Bulgarian NGOs are also using other frameworks and methodologies, elaborated by International Fact-Checking Network and the European Fact-Checking Standards Network. Finally, RESIST Counter Disinformation Toolkit[145], developed by the government of the United Kingdom, was also used by Bulgarian public administration, according to survey respondents.

3.3. Cooperation between state institutions and NGOs

The authors of this report have identified three types of cooperation between public authorities and non-governmental organizations. The first of them is a top-down model where the state institutions animate cooperation with civil society stakeholders. It often translates into formalized cooperation formats established by the relevant institutions. The second type is a bottom-up model where cooperation is initiated by the NGOs. The third model takes the

---

[142] Secrétariat général de la défense et de la sécurité nationale : RAPPORT DU COMITÉ ÉTHIQUE ET SCIENTIFIQUE SUR L'ACTIVITÉ DU SERVICE DE VIGILANCE ET DE PROTECTION CONTRE LES INGÉRENCES NUMÉRIQUES ÉTRANGÈRES (VIGINUM) JUILLET 2021 – DÉCEMBRE 2022, https://www.sgdsn.gouv.fr/files/files/Viginum%20-%20rapport%20CES.pdf [05.06.2024].

[143] *Informacinę erdvę NATO viršūnių susitikimo metu stebėjo pirmą kartą Lietuvoje suburta tarpinstitucinė analitikų komanda*, 14 July 2023, https://lrv.lt/lt/naujienos/informacine-erdve-nato-virsuniu-susitikimo-metu-stebejo-pirma-karta-lietuvoje-suburta-tarpinstitucine-analitiku-komanda/

[144] ATT&CK Matrix for Enterprise, https://attack.mitre.org/.

[145] Government Communication Service, RESIST 2 Counter Disinformation Toolkit, https://gcs.civilservice.gov.uk/publications/resist-2-counter-disinformation-toolkit/.

form not only of non-cooperation but of active obstruction by state institutions of NGOs' activities aimed at tackling disinformation and FIMI.

This typology has been elaborated on the basis of case studies of cooperation models in the member states, including data from expert interviews, surveys and desk research. Below, the characteristics of each model are illustrated with the most emblematic cases.

3.3.1. Top-down cooperation model

Many European Union member states seek to use the advisory and consultative role of NGOs for resilience building, developing comprehensive strategies regarding FIMI and improving strategic communication. How this cooperation is animated depends on various individual considerations in each country. Countering disinformation and foreign interference covers a whole spectrum of activities. However, each country has its own approach to the complex problem of FIMI, focusing on its different aspects, which determine cooperation with civil society actors.

To strengthen the process of best practices exchange between the public administration and the third sector, states often aim to formalize cooperation with civil society organizations and stakeholders. This takes the form of appropriate orders, and provisions in the statutory documents of state bodies and institutions, which then are translated into **formalized cooperation platforms**. One of this report's observables is that the establishment of formalized cooperation platforms with civil society organizations corresponds to the medium and high level of institutionalization of coordination systems in the member states. States that have established such platforms for regular cooperation, coordinated by state institutions are Sweden (assessed as a "champion" with a high level of institutionalization), Finland, Ireland, Italy, Spain, and Poland (assessed as "aspiring players" with a medium level of institutionalization).

Table 3: Formalized cooperation platforms and the coordinating state institution

Member state	**Formalized cooperation platform**	**Coordinating state institution**
Finland	Security Committee	Ministry of Defence
	Knowledge Center on Information Resilience	National Emergency Supply Agency
Spain	Forum against Disinformation Campaigns	Department of National Security of the Cabinet of the Presidency of the Government
Sweden	Cooperative Council	Psychological Defence Agency
Poland	Consultative Council on Resilience to International Disinformation	Ministry of Foreign Affairs
Ireland	The Working Group	Department of Tourism, Culture, Arts, Gaeltacht, Sports and Media

Member state	Formalized cooperation platform	Coordinating state institution
	Media Literacy Ireland	Media Commission
Italy	Technical Table	Communications Regulatory Authority

Source: own study

France was not included in the table, but cooperation between the state institutions and NGOs features a top-down model. Although no official cooperation platform has been established yet, the VIGINUM is in charge of communication with civil society and academia. This is a work in progress and only started in 2023 after initial service consolidation. In 2023 a conference reuniting stakeholders was organized to map relevant actors and as of 2024, these exchanges were supposed to be made more focused and concrete.

Finland established two cooperation platforms. The first one is the Security Committee – an independent, permanent cooperation body for which the Ministry of Defense provides a secretariat[146]. The second one is the Knowledge Center on Information Resilience of The National Emergency Supply Agency, which has broadened its scope on hybrid threats and informational influence.[147]

Poland established the Consultative Council on Resilience to International Disinformation in September 2024, as an advisory body to the Ministry of Foreign Affairs. It is composed of a chairperson (Plenipotentiary of the Minister of Foreign Affairs for Countering International Disinformation), his deputy and representatives of civil society invited by the Minister. Experts with knowledge or experience in a specific field may participate in the Council's work as advisors. The Council meet at least every two months, or more often if required[148]. The idea of a resilience council was championed by the SAUFEX consortium.

Spanish Forum against Disinformation Campaigns, gathering experts from different civil society sectors, meets once a year to discuss potential areas to tackle for the next 12 months based on the current trends and threats. In December 2022 9 working groups were established, with a visibly greater attention attached to foreign interference driven by the Russian invasion of Ukraine.

---

[146]Fjäder, C. & Schalin, J. *Building resilience to hybrid threats: Best practices in the Nordics*. The European Centre of Excellence for Countering Hybrid Threats (HybridCoE). [date published: May 2024] https://www.hybridcoe.fi/wp-content/uploads/2024/05/20240527-Hybrid-CoE-Working-Paper-31-Building-resilience-to-hybrid-threats-WEB.pdf , p. 18..
The Security Committee of Finland/Turvallisuuskomitea. *Operation and Responsibilities*. [last accessed: 02.08.2024] https://turvallisuuskomitea.fi/en/security-committee/operation/

[147] Finnish National Emergency Supply Agency/Huoltovarmuuskeskus. *Countering information influencing - Preliminary report/Informaatiovaikuttamisen torjunta - Esiselvitys*. [date published: 01.12.2021]. https://www.huoltovarmuuskeskus.fi/files/d601de13993e8873d2d66bf379c35f13309dc42a/hvk-informaatiovaikuttamisen-torjunta-esiselvitys.pdf; Finnish National Emergency Supply Agency/Huoltovarmuuskeskus. *Finnish National Emergency Supply Agency builds capabilities to counter information influencing/ Huoltovarmuuskeskus rakentaa kykyä torjua informaatiovaikuttamista.* [date published: 17.08.2022] https://www.huoltovarmuuskeskus.fi/a/huoltovarmuuskeskus-rakentaa-kykya-torjua-informaatiovaikuttamista#

[148] *Zarządzenie nr 30 Ministra Spraw Zagranicznych w sprawie Rady Konsultacyjnej do spraw Odporności na Dezinformację Międzynarodową przy Ministrze Spraw Zagranicznych*, Warsaw 11.09.2024, https://www.gov.pl/web/dyplomacja/zarzadzenie-nr-30-ministra-spraw-zagranicznych-z-dnia-11-wrzesnia-2024-r-w-sprawie-rady-konsultacyjnej-do-spraw-odpornosci-na-dezinformacje-miedzynarodowa-przy-ministrze-spraw-zagranicznych [Access: 29.10.2024].

Italy's Technical Table (*Tavolo tecnico*) brings together media representatives, digital platforms, academics and civil society stakeholders. Work is carried out in 4 thematic groups: telecommunications and consumers, postal services, media services and digital platforms[149], and big data.

Based on the type of coordinating state institution, we can distinguish two patterns. First, cooperation may be coordinated by institutions that are part of the national security sector (MFA, MoD, etc.). This is the case for the majority of the EU member states and indicates that those countries frame FIMI mainly as a security problem. The second pattern was detected in Ireland and Italy. In Ireland, there is emphasis on the media sector and promoting media literacy. In Italy, the cooperation platform is coordinated by a regulatory institution, which shows a more technical approach to FIMI.

Another form of top-down cooperation type is **state funding of research projects regarding disinformation**, notably in Austria, Croatia and Germany. The central focus of Austrian research projects are deep fakes. The Federal Ministry of Finance is responsible for funding research and development initiatives related to security and defense. This includes funding projects to identify and combat disinformation e.g. DefalsifAI project[150]. In Croatia, state financing is provided for universities in a public call by the Ministry of Culture and Media and the Agency for Electronic Media[151]. Germany has pledged to invest in research on the impact of FIMI on democracies as a member of G7 format. It supports the call for access to data for researchers to better understand the scope, scale and extent of information manipulation.

Estonia, Latvia and Lithuania are examples of small countries that boost their institutional capacities by cooperating with various third-sector actors in the field of combating FIMI. As a result of the peculiarities of small countries, the community of people and organizations involved in countering disinformation is not sizeable. Experts know each other, which translates into more **informal**, but vibrant forms of **cooperation and information exchange**. In Lithuania the NGOs are included in the operational algorithm of intervention of the National Crisis Management Center (NCMC) responsible for strategic communication and response to informational threats. The NCMC recommends NGOs respond to an incident, when the threat level is low (3-5 out of 10), according to the scale used by this institution[152].

3.3.2. Bottom-up cooperation model

The bottom-up cooperation is when activities are initiated by third-sector stakeholders, while the state institutions remain passive. Accordingly, no formalized mechanisms and formats exist for cooperation between the public sector and NGOs. The bottom-up model of cooperation can be identified in states with relatively low institutional capacity, often facing political and social challenges, where NGOs complement state capacities or compensate for their absence. No formalized and permanent cooperation formats with civil society were identified in countries with low levels of institutionalization. States with bottom-up cooperation model are *inter alia* Belgium, Romania and Bulgaria, where our respondents assessed the level of cooperation between the public and third sector as rather low.

---

[149] Example of public consultations on regulations regarding removing malicious online videos: https://web.archive.org/web/20230509160315/https://www.agcom.it/documents/10179/29559719/Delibera+22-23-CONS/1e92c9c1-53fb-4229-b92a-ca91613a42d4?version=1.0

[150] Defalsif-AI, Austrian Presse Agentur, https://science.apa.at/project/defalsifai-en/

[151] Read-Twice-Media-Literacy-Needs-Assessment-CROATIA-v1.pdf (echo-udruga.hr)

[152] *955 Dėl Strateginės Komunikacijos Nacionalinio Saugumo Srityje Koordinavimo Tvarkos Aprašo Patvirtinimo*, https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/3f019ef4eb8511eab72ddb4a109da1b5?jfwid=2r1mkfzc.

In particular, the NGOs seek to engage with the public administration by inviting the officials to various events, preparing proposals for legislation, conducting training for civil servants, promoting analytical and digital tools and frameworks, and sharing best practices. Often these are organizations that are part of the EDMO network.

In Belgium, due to the country's regional and linguistic fragmentation, national-level initiatives are scarce. However, the *Centre de Crise National* (NCCN: National Crisis Centre) promotes research and tools developed by NGOs. The organizations mentioned include notably EDMO BELUX and DROG. Despite initiating cooperation, NGO experts from Romania indicate passiveness of state institutions and lack of real effects. This translates further into a lack of effective public debate on how the state should tackle disinformation and conduct strategic communications. In Bulgaria, protracted political instability is not conducive to enhancing permanent cooperation and implementing the NGOs' recommendations. However, Bulgarian NGOs contributed to initiation of bilateral cooperation on matters related to FIMI between the US' and Bulgaria's administrations. Moreover, on the occasion of organized events, they enhance the exchange of practices between Bulgarian administrative representatives and representatives of institutions such as VIGINUM and the European Commission. The NGOs also promote the DISARM, STIX and OpenCTI tools, providing training for administrative staff.

3.3.3. Non-cooperation (obstruction) model

There is a group of member states where state institutions and civil society are not only completely decoupled, but the state actively limits the capacities of NGOs to investigate and counter disinformation. This pattern is discernible in Slovenia, Slovakia and especially in Hungary.

Hungarian civil society organizations, which receive funding from foreign sources, are considered by the government as foreign agents of influence. In addition, the Hungarian government considers European funds as a foreign source of funding. This approach is illustrated by the Sovereignty Protection Act adopted in November 2023[153]. The purpose of this law is not entirely clear, but it targets independent institutions (NGOs and media), which draw funding from Western foreign sources. This is similar to the Russian Foreign Agents Act, which classifies Western soft power as a threat. Pinning the "foreign agent" label on independent organizations undermines public trust in them. Another action to limit civil society's capacities is restricting access to information for independent journalists and NGOs. Fees for accessing relevant public information are being increased and state institutions are granted ever more time to provide it[154]. Moreover, Hungary simulates cooperation with civil society on FIMI, by establishing a network of state-controlled GONGOs and institutions, such as V4 News Agency branded as independent, yet in reality funded by government politicians[155].

---

[153] J. Wiseman, S. Panyi, *MFRR Podcast: Navigating Hungary's new Sovereignty Protection Act*, 31.10.2023, International Press Institute, https://ipi.media/ipimedia/mfrr-podcast-navigating-hungarys-new-sovereignty-protection-act/ [Access: 02.08.2024].

[154] *The Hungarian government further weakens freedom of information and transparency*, DemNet 11.06.2019, https://demnet.hu/en/blog-en/hungarian-government-further-weakens-transparency/ [Access: 22.09.2024]; J. Munkacsoport, *Hungarian government further weakens access to information*, K-Blog 23.01.2024, https://k.blog.hu/2024/01/23/hungarian_government_further_weakens_access_to_information?utm_medium=doboz&utm_campaign=bloghu_cimlap&utm_source=nagyvilag [Access:22.09.2024].

[155] M. Sarkadi Nagy, *London-based V4 Agency is Orbán's propaganda machine disguised as global media product*, „Atlatszo.hu", 25.05.2020, https://english.atlatszo.hu/2020/05/25/london-based-v4-agency-is-orbans-propaganda-machine-disguised-as-glob

4. International cooperation: exchange of best institutional practices

The bilateral and multilateral international cooperation on countering FIMI allows to exchange best institutional practices and enhances mutual capabilities. It often takes the form of creating institutions, which serve as platforms for multilateral cooperation. The authors of this report identified two types of best practices flows: the vertical flow (organization to state) and the horizontal flow (state to state and organization to organization).

This analysis is based on open-source data and opinion of interviewed experts. Due to security concerns and political sensitivities related to FIMI, not all details of international cooperation are public. However, the EU member states' engagement and cooperation in international organizations and with other states reflect their strategic interests, foreign policy goals and individual considerations, as well as the level FIMI threat perception. For example, Latvia's diverse modes of international cooperation include the EU, the United Nations (UN), Council of Europe (CoE), the Organization for Security and Cooperation in Europe (OSCE), and the Organization for Economic Cooperation and Development (OECD), as well as various bilateral and regional formats. Italy in turn sees its engagement in countering disinformation within G7 and the OECD as an opportunity to exert global influence in this field.

3.4.1. Vertical flow of best practices (organization to state)

The vertical flow of best practices is understood here as a process where solutions and mechanisms developed within international organizations such as the EU, NATO and OECD are transferred to individual countries.

European Union

EU institutions and member states share insights related to disinformation campaigns and coordinate responses through the Rapid Alert System (RAS). Especially, but not exclusively, the EU is viewed as a norm-setter of good practices in the Netherlands, Sweden, Finland Austria, Poland, France, Romania, Germany and Estonia. In France, VIGINUM contributes significantly to expanding pan-European situational awareness by supplementing the RAS database. The Polish MFA engages in international cooperation on countering disinformation through policy making at the EU–level, involving the FIMI toolbox, sanctions, pro-active media campaigns, and funding small-scale projects countering FIMI. Estonia and Germany participate in the work of the Task Force on Eastern Strategic Communication of the European External Action Service (EEAS) with a seconded expert.

NATO

Under the NATO umbrella, Member States cooperate to enhance their capabilities, notably within Centers of Excellence (COEs), created and funded at the initiative of individual countries. COEs are international military organizations that train and educate leaders and specialists from NATO member and partner states. Although they are NATO-accredited, they are not part of the NATO Command Structure, nor subordinate to any other NATO entity.

---

al-media-product/ [Access: 01.08.2024]; S. Walker, *London media agency carries Viktor Orbán's nativist message*, „The Guardian", Budapest 5.05.2019, https://www.theguardian.com/world/2019/may/05/london-based-media-agency-channels-victor-orban-nativist-message-hungary [Access: 01.08.2024]; M. Sarkadi Nagy, *"International News Agency" informing Hungarians about a declining West from London has actually never left Budapest*, „Atlatszo.hu", 8.09.2022, https://english.atlatszo.hu/2022/09/08/international-news-agency-informing-hungarians-about-a-declining-west-from-london-has-actually-never-left-budapest/ [Access: 01.08.2024].

The NATO Strategic Communication Centre of Excellence is based in Riga, Latvia. It was established in 2014 by Latvia, Estonia, Germany, Italy, Lithuania, Poland, and the United Kingdom, later joined by Sweden, Netherlands, Finland, Slovakia, Denmark, Hungary and Spain. It functions as a multi-stakeholder platform, supported by international experts with military, government or academic background, contributing to the strategic communication capabilities of participating countries.

Estonia and Romania build their counter-FIMI capabilities by actively engaging in cybersecurity cooperation within NATO and the EU. This is reflected in the establishment of the NATO Cooperative Cyber Defense Centre of Excellence and the EU Agency for Large-scale IT Systems (EU-LISA) in Tallinn. Romania relies heavily on cooperation with the EU and NATO. With its traditionally greater emphasis on cybersecurity, Romania very much follows approaches developed by its NATO partners when it comes to countering disinformation. Also Sweden sees its newly-acquired NATO membership as an important platform to pursue the issue of disinformation and notes the importance of EU - NATO cooperation in countering hybrid threats in general[156].

Noteworthy is the European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE) – an autonomous organization, which is the only multilateral framework, where the EU and NATO, as well as G7 members, work and conduct exercises together. The Centre's work is planned and coordinated by the Hybrid CoE Secretariat, located in Helsinki, Finland. Participation in the Centre's activities is open to all EU and NATO countries, and the number of Participating States has grown to include 36 today. It acts as a think tank, expert and advisory support, and a platform for sharing experience and information on hybrid threats (including FIMI). The Helsinki centre primarily contributes to the situational awareness of both organisations by providing expertise and training for countering hybrid threats[157].

OECD

Another relevant cooperation forum is the OECD Information Integrity Hub established in 2022 as a peer-learning platform, enabling countries to exchange data and best practices. The initiative is supported notably by France, Belgium, Finland, Greece, Italy, Lithuania, Luxembourg, the Netherlands and a few non-EU countries (Korea, Chile, Colombia, Canada, the UK, the US, and Norway). The Hub also functions as the Steering Group of the OECD Expert Group on Public Governance Responses to Mis- & Disinformation composed of all OECD member countries[158].

3.4.2. Horizontal flow of best practices (state to state and organization to organization)

The horizontal flow of best practices is understood here as a process where solutions and mechanisms are exchanged between individual states (bilateral cooperation) and regional formats (multilateral cooperation). The latter may notably include cooperation within such minilateral formats as the Weimar Triangle, the Lublin Triangle, the Baltics or Benelux states.

By sharing their know-how on countering FIMI, more advanced states help to strengthen the capabilities of newcomers to this policy area. The most active players in terms of providing such assistance are the United Kingdom, which exports its strategic communication model, and France, which promotes VIGINUM's institutional and operational model of countering

---

[156] Government Offices of Sweden/Prime Minister's Office. *National Security Strategy.* [date published: July 2024]. https://www.government.se/globalassets/government/national-security-strategy.pdf, p. 28, 29.
[157] For more, see: https://www.hybridcoe.fi/who-what-and-how/.
[158] OECD Information Integrity Hub, https://www.oecd.org/en/networks/oecd-information-integrity-hub.html [Access: 24.10.2024].

FIMI. The United States also have its framework of cooperation with like-minded countries (see below).

France is an exporter of good practices to countries seeking guidance in building their institutional potential. The VIGINUM's Coordination and Strategy Unit is in charge of international relations, both bilateral and multilateral, aimed at positioning France as a key actor within the community that fights FIMI. Consultations with VIGINUM experts were held notably in Bulgaria and Germany, the latter following the French model in designing its agency to combat disinformation.

A format for transatlantic cooperation is the US Framework to Counter Foreign State Information Manipulation. It serves as a tool for diplomatic engagement and to deepen the cooperation between like-minded partners. In 2024 eight EU member states (Poland, Bulgaria, Romania, Finland, Estonia, Lithuania, Czechia and Italy) signed a memorandum of understanding to strengthen cooperation with the United States on countering foreign state information manipulation. Importantly, six of them are NATO "eastern flank" states.

Bulgaria is an example of a country that seeks assistance and guidance from partners (notably the US and UK) on developing institutional capacity and formal legal solutions to counter FIMI. State institutions such as MFA and MoD use the British RESIST framework in their work, which is the base model adopted by the Bulgarian administration. Bulgaria is in the initial phase of building its capacity, and the RESIST toolkit is mostly adopted as a starter model for fledgling countries.

In addition, collaboration on tackling FIMI intersects across organizations and formats. For example, the European Union cooperates with the G7 in the Rapid Response Mechanism (RRM), coordinated by Canada, and with NATO[159].

As to EU-NATO cooperation, NATO officials indicated that due to political reasons and a lack of agreement on the exchange of classified information, it is relatively narrow. The mandate of the NATO Public Diplomacy Division (NATO PDD) is mostly to carry out the Alliance's public communications and communicate its aims and objectives. Thus, NATO as an organization is quite limited in terms of countering FIMI and most activities are within the responsibility of the member states. Exchange of views between the two organizations does not always translate into real actions and their implementation at the national level. However, the potential for cooperation between NATO and EU lies in the standardization of detection, analysis and response methods to FIMI and ensuring interoperability[160].

A noteworthy group in the EU are G7 members: Italy, Germany and France. The Group member states host numerous so-called very large online platforms and search engines (VLOPs and VLOSEs)[161], which is significant for their role as norm-setters in tackling disinformation. Policy guidelines set in the G7 on a specific topic often have a "ripple effect" in many other international organizations and institutions. For instance, in 2018 the G7 established the Rapid Response Mechanism (RRM) dedicated to strengthening coordination, analysis and response to information threats. This tool is part of the broader G7 Commitment

[159] *Disinformation and Foreign Interference: Speech by High Representative/Vice-President Josep Borrell at the EEAS Conference*, Brussels 21.01.2024, https://www.eeas.europa.eu/eeas/disinformation-and-foreign-interference-speech-high-representativevice-president-josep-borrell-eeas_en [Access: 21.10.2024]

[160] Saufex study visit to NATO headquarters in Brussels, 23.04.2024.

[161] Very large online platforms and search engines are those with over 45 million users in the EU. They must comply with the most stringent rules of the DSA.

to Defending Democracy from Foreign Threats[162]. Meetings of the RRM Working Groups are held with the participation of representatives of NATO, EU, OECD, think tanks, civil society stakeholders and institutions such as EDMO branches and companies like Google[163]. During Italy's 2024 presidency in G7 AI-generated disinformation is under the spotlight[164].

To sum up, countries, which experienced hybrid attacks in the past, are more likely to engage in various international initiatives and cooperation formats to strengthen their security. They see membership in EU, NATO or OECD and bilateral formats as a platform to pursue thematic issues, including disinformation. The "trendsetters" are notably Baltic states, Finland, Poland, Sweden, as well as G7 countries - Italy, France and Germany. However, those states that do not feel particularly threatened, tend to follow trends occurring in international fora. The "followers" countries are inter alia Belgium, Romania and Bulgaria.

The main push factor that led to increased international cooperation and boosting of institutional capabilities on FIMI was predominantly the Russian Federation's aggressive behavior in Europe and beyond, in particular the full-scale invasion of Ukraine. In addition, hybrid attacks on Polish-Belarussian and Lithuanian-Belarussian border orchestrated by Belarussian authorities with Russian support, provided for important policy triggers for both Poland and Lithuania. Lithuanian FIMI-related capabilities were strengthened in view of the 2023 NATO summit in Vilnius and expected hostile actions from Russia. Some eastern flank countries, notably Estonia, have a longer history of dealing with Russia-orchestrated hybrid threats, starting with cyber-attacks on its critical infrastructure conducted as early as 2007. Beyond Central and Eastern Europe, the French experience of foreign interference in presidential elections in 2017, as well as FIMI campaign directed at the French Army in Mali in 2022, proved vital for both creating an exemplary national-level coordination system and engaging in international cooperation as best-practice exporter. Yet other countries, disposing of relatively limited administrative capacities, such as Romania, chose to follow the path already outlined by NATO allies.

3.5. Conclusions

EU member states' coordination systems aimed at countering FIMI reveal differentiated levels of institutionalization. Only two member states (France and Sweden) can be qualified as "champions" of institutionalization, featuring centralized systems of coordination, with government-level coordination mechanism and established specialized agencies responsible for FIMI identification, analysis and response. A larger group of "aspiring players" consists of big member states (Germany, Italy, Poland and Spain), as well as small Northern and Eastern European states (notably Estonia, Finland, Lithuania), directly and repeatedly targeted by Russian hybrid threats, including FIMI. These states dispose of decentralized coordination systems, with either government or ministerial level coordination mechanism, whereas some of them (Germany and Finland) already experiment with specialized-agency type of solution. However, many states across the entire EU are still characterized by low level of institutionalization (laggards), featuring only a rudimentary decentralized coordination system with coordination mechanism at sectoral level or no proper coordination system at all. Low

---

[162] *Charlevoix Commitment on Defending Democracy from Foreign Threats*, Charlevoix 2018, https://publications.gc.ca/collections/collection_2018/amc-gac/FR5-144-2018-30-eng.pdf [Access: 23.10.2024].

[163] For example: *G7 Working Group Meeting on disinformation at the Farnesina*, 3.07.2024, https://www.esteri.it/en/sala_stampa/archivionotizie/comunicati/2024/07/riunione-alla-farnesina-del-gruppo-di-lavoro-g7-su-disinformazione/ [Access: 24.10.2024].

[164] L. De Agostini, B. Catena, S. Autolitano, *Mitigating AI-Generated Disinformation: A Cyber Collaborative Framework for G7 Governance*, Policy Brief, Think7, May 2024, https://think7.org/wp-content/uploads/2024/05/T7it_tf1_pb01.pdf [Access: 23.10.2024].

level of institutionalization correlates with small size of the state, limited administrative capacities, and low level of perceived FIMI threat.

Accordingly, there is limited evidence as to the use of analytical frameworks, such as DISARM, and digital tools, such as STIX and Open CTI, across the EU member states' institutions. This results, on one hand, from little information being shared in the public domain due to security concerns and political sensitivities, and on the other hand, from genuinely limited use of these tools to date. France – an institutionalization "champion" – is a rare example of a member state that is both an advanced and transparent user. One may conclude that there is a clear need for more information and best practice sharing in this respect, both between member states, and state institutions and civil society.

Three models of cooperation of state institutions with civil society organizations were identified: a top-down cooperation model, a bottom-up cooperation model, and a non-cooperation model. A top-down model, with its formalized cooperation platforms (Finland, Ireland, Italy, Poland, Spain, Sweden), correlates with medium to high level of institutionalization of coordination systems. Meanwhile, bottom-up (Belgium, Bulgaria and Romania) and non-cooperation (Hungary) models correlate with low level of institutionalization of coordination systems.

With regard to international exchange of best institutional practices, a correlation was found between active engagement in international cooperation and previous experience of major hybrid attacks, including FIMI. Two types of flows of best practices on countering FIMI were identified: vertical flow (organization to state) and horizontal flow (state to state and organization to organization). The vertical flow was identified notably within the EU, the OECD, and NATO. As to the horizontal flow, EU member states with medium to high level of institutionalization of coordination systems (France) or former member states (United Kingdom) act as trendsetters and exporters of best practices. In addition, non-EU allies, such as US, create their own tools of multilateral engagement aimed, in particular, at EU and NATO eastern flank members. Meanwhile, states that have not experienced major hybrid attacks and/or states with relatively limited administrative capacities, and thus with low level of institutionalization of coordination systems, tend to be followers and importers of best practices. Horizontal flows were also identified between organizations and formats, notably between EU and NATO or EU and G7.

Part IV – REGULATIONS

Agnieszka Legucka, Piotr Sosnowski

4.1. Overview

None of the European Union Member States has specific legislation dealing directly with FIMI. States make use of various criminal offenses that can be used to combat the phenomenon of disinformation (e.g. defamation, insult, misleading a public institution or public promotion of fascism and hate speech, hooliganism). Given the different legal cultures of the countries of the European Union, research carried out as part of the SAUFEX project shows that the regulation of the fight against FIMI depends on the model of state intervention in the information sphere adopted. An analysis of the legal regulation of disinformation in EU Member States allows four levels of legislative interference to be distinguished. The **minimal** interference model, mainly represented by Luxembourg, is characterised by a deliberate abandonment of dedicated legislation and a wait for European regulation[165]. Luxembourg law does not define information manipulation or external interference[166], as does Czech law, where attempts at regulation have failed due to the lack of an adequate legal basis, as confirmed by the courts there.

The model of **moderate** interference, seen in Austria and Portugal, is based on using **the existing legal framework** without creating specific legislation. Austria adapts current media regulations and rectification mechanisms, while Portugal has introduced legislation under the Charter on Human Rights in the Digital Age, but without defining specific sanctions for the spread of disinformation. Denmark also belongs to this group, regulating the issue through a ban on political advertisements on television and a media liability regime. And the Netherlands, whose approach is characterised by a particular focus on regulating political advertising through a **voluntary** code of conduct (*Gedragscode Transparantie Online Politieke Advertenties*). This model seen in Austria, Belgium, and Italy, is mainly based on the classic instruments of criminal law (defamation, incitement to hatred) and media law, supplemented by mechanisms to control online content. Also Finland does not have national laws specifically against disinformation or FIMI, relying more on media education and existing laws.

Significant interference characterises the approaches of Germany and France. Germany's NetzDG law requires social media platforms to **remove illegal content** within 24 hours of notification[167], while France's ARCOM has broad coordination powers and can impose **fines** of up to 6% of platforms' global turnover[168]. Particularly relevant are the French regulations for the pre-election period, allowing a rapid response to disinformation.

The most **intense** interference is observed in the Baltic States and Poland, due to their geopolitical location and historical experience. Lithuania has criminalised social media

---

[165] Nicolas Hénin & Maria Giovanna Sessa, *Disinformation Landscape in Luxembourg*, op. Cit.

[166] Belgium – Luxembourg Digital Media and Disinformation Observatory, Regulating disinformation: look-up on the legal framework in Luxembourg, op. cit.

[167] *Gesetz zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken (Netzwerkdurchsetzungsgesetz - NetzDG)*, https://www.bundesjustizamt.de/SharedDocs/Downloads/DE/Hasskriminalitaet/20220721_NetzDG.pdf?__blob=publicationFile&v=2.

[168] Amélie Blocman, PLATFORM REGULATION AND DSA IMPLEMENTATION: ARCOM AND EUROPEAN COMMISSION INCREASE COOPERATION, IRIS Legal Observations of the European Audiovisual Observatory, https://merlin.obs.coe.int/article/9903.

manipulation with a penalty of up to **five years in prison**[169], Latvia has adopted similar measures in the context of elections and deepfake technology. Poland has introduced the harshest penalties - a minimum of **eight** years' **imprisonment** for **disinformation carried out on behalf of foreign intelligence**.

In this context, the case of Cyprus is interesting, whose existing legislation (Article 50 of the Penal Code) criminalises the classic offence of publishing false news, focusing on the intention to cause fear and public alarm – punishable by a fine and up to two years' imprisonment[170]. A key element is the offender's awareness of the falsity of the information ('knows or has reason to believe it to be false'), which makes it difficult to penalise the sharing of already existing false content. The new law (planned for September 2024) is expected to criminalise 'fake news' explicitly, with a penalty of up to 5 years' imprisonment[171].

4.2. Legislation of the EU's Member States

Based on an analysis of EU documents – the Strengthened Code of Practice on Disinformation 2022 and the European Commission Guidance on Strengthening the Code of Practice on Disinformation – six key regulatory variables in the area of countering disinformation can be distinguished. The primary variable is the presence of dedicated legislation that directly addresses disinformation, underpinning the legal framework in this area. The second variable concerns the implementation of the DSA, which introduces binding legal obligations for online platforms and establishes a co-regulatory framework. The third variable is the regulation of political advertising, which is crucial for the transparency of democratic processes and against the manipulation of public opinion. The fourth variable relates to the legal framework for access to data for researchers and fact-checkers, which is important for monitoring and analysing disinformation phenomena. The fifth variable includes oversight and enforcement mechanisms that ensure the effectiveness of adopted regulations. The last variable is the criminal legislation on disinformation, which is a deterrent and sanctioning element. These variables form a comprehensive regulatory framework to assess the degree of development of legal instruments in individual EU Member States to counter disinformation.

Table 4: Implementing the EU Code of Conduct on Disinformation

State	Dedicated Legislation	Political Advertising Regulation	Criminal Provisions	Media Authority	DSA Coordinator	Other Key Authorities

[169] *Anyone who, by manipulating the accounts of an online social networking service platform, significantly increased the dissemination of information aimed at acting against the Republic of Lithuania [...] shall be liable to [...] imprisonment for up to five years*,

[170] Cyprus Criminal Code. [last accessed 14.07.2024], https://www.cylaw.org/nomoi/arith/CAP154.pdf, p. 27
European Regulators Group for Audiovisual Media Services (ERGA). *Notions of disinformation and related concepts (ERGA Report),* 2021. https://erga-online.eu/wp-content/uploads/2021/03/ERGA-SG2-Report-2020-Notions-of-disinformation-and-related-concepts-final.pdf, p. 33, 69.

[171] Cyprus Mail. *Freedom of speech objection to fake news criminalisation push.* [date published: 04.07.2024]. https://cyprus-mail.com/2024/07/04/freedom-of-speech-objection-to-fake-news-criminalisation-push/
Verfassungsblog. *Prison for Fake News: A Proposal to Criminalize Fake News in Cyprus.* [date published: 12.07.2024]. https://verfassungsblog.de/prison-for-fake-news/

Austria	No, but has relevant provisions in Media Act	Yes, through Media Act	Yes (§§ 105f StGB and others)	KommAustria	KommAustria	Federal Communications Senate (appeals body)
Belgium	No	Yes, through general media law	Yes (general criminal law)	CSA (Fr.), VRM (Fl.)	FPS Economy (planned)	Intelligence Services Review Committee
Bulgaria	No	Limited	No specific provisions	Council for Electronic Media (CEM)	Communications Regulation Commission (CRC)	-
Croatia	No	Yes, through media law	Limited	Agency for Electronic Media (AEM)	HAKOM	-
Cyprus	Planned (2024)	Limited	Yes (Article 50 Penal Code)	Cyprus Radiotelevision Authority	Cyprus Radiotelevision Authority	-
Czech Republic	No	Limited	No specific provisions	RRTV	Czech Telecommunication Office	-
Denmark	No	Yes[172]	Yes (§108 Criminal Code)	Radio and Television Board	Danish Business Authority	Media Liability Board
Estonia	No	Through general media law	Yes (§280 Criminal Code)	CPTRA	CPTRA	-
Finland	No	Yes	Yes (Criminal Code)	TRAFICOM	TRAFICOM	-
France	Yes (Law 2018-1202)	Yes, comprehensive	Yes	ARCOM	ARCOM	VIGINUM (foreign digital interference)
Germany	Yes (NetzDG)	Yes	Yes (StGB)	The Media Authorities (*die medienanstalten*)[173]	Federal Network Agency (BNetzA)	Federal Office for Information Security, Central Office for the Recognition of Foreign Information Manipulation (ZEAM)
Greece	No	Limited	Limited	NCRTV	EETT	-

[172] The Danish law interprets 'political' in a broader sense than only party politics, but refers also to campaigning for the purposes of influencing legislation or executive action by local or national (including foreign) governments.

[173] The central supervisory authorities for the regulation of private broadcasting and telemedia in Germany is made up of 14 separate offices of the German States. See: https://www.die-medienanstalten.de/

Hungary	No	Limited	Yes (Criminal Code)	NMHH	NMHH	-
Ireland	Yes (Online Safety Act 2022)	Yes (Electoral Reform Act 2022)	Limited	Coimisiún na Meán	Coimisiún na Meán	Electoral Commission
Italy	No	Yes, through AGCOM guidelines[174]	Yes (Article 656)	AGCOM	AGCOM	Agenzia per la Cybersicurezza Nazionale ACN
Latvia	No	Limited	Yes (Article 231)	NEPLP	Consumer Rights Protection Centre	-
Lithuania	Yes	Yes	Yes (Article 285)	LRTK	RRT	Strategic Communication Department
Luxembourg	No	No	No	ALIA	Competition Authority	-
Malta	No	Limited	Yes (Article 82)	Broadcasting Authority	MCA	-
Netherlands	No	Yes, comprehensive	Yes (Criminal Code)	CvdM	ACM	-
Poland	No	Limited	Yes (Article 130(9))	KRRiT	UKE (planned)	Internal Security Agency
Portugal	Yes (Law 27/2021)	Limited	No	ERC	ANACOM	-
Romania	No	Limited	Yes (Article 404)	CNA	ANCOM	-
Slovenia	N/A	N/A	N/A	AKOS	AKOS	-
Spain	Yes (PCM/1030/2020)	Yes	Indirect provisions	CNMC	No data available	Permanent Commission against Disinformation
Sweden	No	Yes, comprehensive	Yes (Criminal Code)	MPRT	Post and Telecom Authority	Swedish Psychological Defence Agency

Source: *Audiovisual Regulators*, European Commission**,** https://digital-strategy.ec.europa.eu/en/policies/audiovisual-regulators [accessed: 10.11.2024]; Digital Services Coordinators, European Commission, https://digital-strategy.ec.europa.eu/en/policies/dsa-dscs [accessed: 10.11.2024].

[174] Autorità per le Garanzie nelle Comunicazioni, *Comunicato stampa 16 novembre 2017*, 16.11.2017, https://www.agcom.it/comunicazione/comunicati-stampa/comunicato-stampa-16-novembre-2017, p. 2-3. Autorità per le Garanzie nelle Comunicazioni, *Linee guida per la parità di accesso alle piattaforme online durante la campagna elettorale per le elezioni politiche 2018*, 31.01.2018, https://www.agcom.it/node/11720, [accessed: 27.06.2024].

A comparison of legal regulation against disinformation in EU Member States reveals a significant diversity of legislative approaches. Dedicated legislation exists in several countries: France (Law No. 2018-1202), Spain (PCM/1030/2020), Portugal (Law 27/2021), Ireland (Online Safety and Media Regulation Act 2022) and Germany (NetzDG), while most countries rely on adaptations of existing criminal and media laws. The implementation of the DSA is in various stages of implementation, with an important part of the solutions already implemented in France (ARCOM with penalty powers of up to 6% of global turnover). Regulation of political advertising is particularly developed in Denmark (with a ban on political advertisements on television), Sweden and the Netherlands (Gedragscode Transparantie Online Politieke Advertenties). In terms of criminal legislation, the most comprehensive regulations are found in Austria (§§ 105f StGB and others), the Baltic States (with new legislation from 2024 on, inter alia, deep fakes in Lithuania and Latvia) and Poland (Art. 130(9) of the Criminal Code on disinformation in cooperation with foreign intelligence). The analysis suggests significant differences in the approach to the regulation of disinformation between Member States, ranging from comprehensive legal solutions to piecemeal provisions.

Different types of regulation in the EU countries seek to target manipulation of information, disinformation, fake news, deepfakes, and hate speech more directly. States define the need to combat Foreign Information Manipulation and Interference (FIMI) in various ways, addressing concerns such as the protection of public order, national security, individual or institutional reputation, constitutional order, sovereignty, territorial integrity, defence capabilities, economic stability, public health, and personal rights that impact human dignity.

Table 5: Dedicated regulations to fight with FIMI

Reasons for fighting with FIMI	Examples of Countries	Criminal Law: examples
Public order, public peace, public confidence	Italy, Estonia, Latvia, Malta, Greece, and Hungary	**Malta:** "Maliciously spread false news which is likely to alarm public opinion or disturb public good order or the public peace or to create a commotion among the public or among certain classes of the public is considered an offence with the possibility of three-month sentence" Article 82 of Malta's Criminal Code.
State or national security	Romania, Italy, Estonia, Latvia, and Poland	**Poland:** "Whoever, taking part in the activities of a foreign intelligence service or acting on its behalf, conducts disinformation, consisting in disseminating false or misleading information" Article 130(9) of the Penal Code Poland **Estonia:** Submission of false information. §280 specifies that knowingly providing false information to an administrative authority is punishable by a fine of up to 300 units or by detention. If the act is committed to obtain official documents, gain rights, or be released from obligations, and does not meet the criteria for offenses outlined in §§209-213 of the Code, it is punishable by a pecuniary punishment or up to two years' imprisonment. For legal persons, such acts are punishable by fines of up to 2,000 euros or a pecuniary punishment (Penal Code, Estonia)
Individual or institutional reputation	Italy	**Italy:** Publishing or spreading false, exaggerated or tendentious news that may threaten public order (Article 656 the Criminal Code), and defamation, which can be used in cases of spreading false information damaging to the reputation of individuals or institutions (Article 595 the Criminal Code).

Constitutional order, sovereignty, territorial integrity, defense, or economic power	Lithuania	**Lithuania:** "Anyone who, by manipulating the accounts of an online social networking service platform, significantly increased the dissemination of information aimed at acting against the Republic of Lithuania—its constitutional order, sovereignty, territorial integrity, defense, or economic power, shall be liable to a fine or a restriction of liberty, or to arrest, or to imprisonment for up to five years. (Article 118)" (since 2024, Criminal Code)
Personal rights that impair a natural person in their human dignity	Austria	**Austria:** The Criminal Code §§ 105f: (severe) coercion; § 107: dangerous threats; § 144: extortion; §§ 146ff: fraud; § 148a: fraudulent data misuse; § 107c: continuous harassment via telecommunication or computer system ("cyberbullying"); §§ 297: slander; § 126a: data damage; § 225a: data falsification; § 293: evidence tampering; § 263: deception in an election or referendum, and § 264: dissemination of false news in an election or referendum.

Source: Own research based on the case study of the SAUFEX project

The Dutch strategy acknowledges that more clarity is needed on the government's role in respect of illegal and harmful material[175]. Article 134 of the Criminal Code encompasses distribution offenses, "Any person who distributes, publicly displays or posts written matter or an image, in which the provision of information, opportunity or means to commit any criminal offense is offered, or has such in store to be distributed, publicly displayed or posted, shall be liable to a term of imprisonment not exceeding three months or a fine of the second category."[176] Article 138ab states on computer trespass that "Any person who intentionally and unlawfully gains entry to a computerised device or system or apart thereof shall be guilty of computer trespass and shall be liable to a term of imprisonment not exceeding one year or a fine of the fourth category." The trespass may be executed via breaching a security measure, a technical intervention, by means of false signals or a false key, or by assuming a false identity. Also, a computer trespass committed via a public telecommunication network shall be a punishable offense. Hate speech laws and regulation prohibiting libel and slander, incitement to hatred, sedition and defamation (articles 113, 119, 137, 261, 262 of the Criminal Code)[177].

In Estonia, the legal framework concerning FIMI and its consequences highlights two key provisions: subsection 6 of §12 of the Public Health Act and §§263 and 278 of the Penal Code. Subsection 6 of §12 of the Public Health Act prohibits the dissemination of information that could be harmful to human health or the environment by any person or entity[178]. This has been particularly relevant during the COVID-19 pandemic, with entities like Elvis Brauer's Mém Cafe being penalized for not adhering to safety measures[179].

Poland in August 2023, introduced new legislation targeting foreign intelligence-linked disinformation. An amendment to the Penal Code, penalises spreading disinformation in

[175] van Hoboken, J. et.al. *The legal framework on the dissemination of disinformation through Internet services and the regulation of political advertising.* The University of Amsterdam, 2019.
[176] The Criminal Code of the Netherlands [translated]. [date published 01.10.2012]. https://antislaverylaw.ac.uk/wp-content/uploads/2019/08/Netherlands-Criminal-Code.pdf, p. 81.
The Criminal Code of the Netherlands in Dutch. [last accessed: 14.07.2024] https://wetten.overheid.nl/BWBR0001854/2024-07-01
[177] Ibidem.
[178] 'THE REGULATION OF FACT-CHECKING AND DISINFORMATION IN THE BALTIC STATES', *Becid* (blog), May 2024, https://becid.eu/results_and_studies/the-regulation-of-fact-checking-and-disinformation-in-the-baltic-states/.
[179] Allik Henry-Laur, Defiant café ordered to close doors, 1.12.2021, https://news.postimees.ee/7398387/defiant-cafe-ordered-to-close-doors

collaboration with foreign intelligence with a minimum eight-year prison term[180]. The new article 130(9) aims to prevent serious disruptions in Poland's system or economy, and to dissuade foreign agents and collaborators from such activities. However, concerns have emerged that the broad definition of disinformation might lead to investigations against journalists and NGOs suspected of foreign ties[181].

A special case represents Hungary, where the lack of political will to counteract disinformation translates into a lack of proper legal framework related to it. According to the survey respondentshe only regulations, which have been adopted by state institutions to counter FIMI are **non-binding recommendations** and they are very ineffective, as there were no practical effects of those recommendations like criminal proceedings, financial penalties or blocking of internet domains and accounts.

In the Hungarian legal system, there is no general prohibition on the disclosure of untruths. The Constitutional Court in its interpretations and judgments has indirectly formulated the media's obligation to 'tell the truth'. Ultimately, it imposes on the legislator the obligation to create the conditions for objective and truthful information, when designing the framework within which the media system operates. The constitutional and civil code provisions on the dissemination of untruths mainly concern the context of defamation and freedom of expression[182]. The Criminal Code also refers to slander as „false publication orally or in any other way tending to harm a person's reputation in connection with his professional activity, public office or public activity; or libellous, before the public at large". Moreover, according to the Code false information and untrue statements are punishable if they violate public order or disturb the public peace (Scaremongering and Threat of Public Endangerment)[183].

An important element of the European legal landscape in the fight against disinformation is the varying pace and extent of implementation of EU regulations. While some countries, such as Luxembourg, deliberately hold back their own regulations while waiting for European solutions, others are actively developing national legal mechanisms. Particularly evident are differences in the approach to institutional oversight – from the centralised French model with ARCOM having broad powers, to more dispersed systems as in Belgium. There is also a clear trend in the evolution of legislation to counter new technological threats – examples are the Latvian legislation on deepfakes in the electoral context or the Lithuanian regulation relating to the manipulation of social media accounts. Significant differences can also be seen in the approach to enforcement – from the restrictive German model (NetzDG) requiring removal of illegal content within 24 hours, to softer solutions in other countries. Also noteworthy is the development of specialised institutions such as the Swedish Psychological Defence Agency, the French VIGINUM dealing with foreign digital interference, and German Central Office for the Recognition of Foreign Information Manipulation (ZEAM) indicating a growing professionalisation in the approach to combating disinformation.

4.3. Regulations of media and internet (DSA)

[180] Kancelaria Sejmu. Obwieszczenie Marszałka Sejmu Rzeczypospolitej Polskiej z dnia 7 grudnia 2023 r. w sprawie ogłoszenia jednolitego tekstu ustawy – Kodeks karny (Dz. U. 2024 poz. 17).

[181] T. Wahl, *Rule of law developments in Poland:* May-October 2023, Eucrim, https://eucrim.eu/news/rule-of-law-developments-in-poland-may-october-2023/ [date published: 14.11.2023].

[182] *G. Polyák, Freedom of Speech and the Regulation of Fake News in Hungary: A Legal Fight against State-Generated Disinformation? [in:] Freedom of speech and the regulation of fake news, Intersentia, Cambridge, UK 2023*

[183] *Act C of 2012 on the Criminal Code*, 2012, Section 227, Section 337/1, Section 338, https://www.refworld.org/legal/legislation/natlegbod/2012/en/78046 [Access: 01.08.2024].

The most common practices to regulate FIMI are legislations that cover the media and internet (i.e. Poland, Estonia, Ireland, Germany, Cyprus, Belgium, Romania, Austria, Italy, Netherlands, Luxemburg, Spain, Portugal, and France), and advertising (i.e. Latvia, Netherlands, Portugal, France). For example, in Spain, the General Audiovisual Communication Law (2022) article 10 states that all media and media organizations shall "take measures for the acquisition and development of media literacy skills in all sectors of society, for citizens of all ages and for all media, and will regularly assess progress made" aiming to "enable citizens (…) to use the media effectively and safely, to access and critically analyze information, to discern between fact and opinion, to recognize fake news and disinformation processes and to create audiovisual content responsibly and safely."[184] Such regulation provides for charging media organizations with (partial) responsibility for developing media literacy skills among Spanish citizens.

In Estonia, "Amendments to the Media Services Act", effective from March 9, 2022, impose obligations on video-sharing platforms to remove content inciting hatred, violence, discrimination, or depicting child pornography, contributing indirectly to the combat against disinformation[185]. Another example is "The Electronic Mass Media Law" in Latvia, which restricts foreign media, and undermines national integrity. After Russia invaded Ukraine, Latvia banned Russian TV channels based on these provisions. Article 26 prohibits content such as pornography, violence, calls for war, and content endangering public health. During the Covid-19 pandemic, fines were issued for false claims about the virus. Article 24(4) of the Electronic Mass Media Law mandates that media must report facts fairly, objectively, and neutrally, separating opinions from news. This aims to combat propaganda but risks state interference in journalistic content. In 2023, the National Electronic Mass Media Council fined TVnet for not challenging an interviewee's controversial statement. This raised concerns about state overreach in defining journalistic standards.

One of the general regulations that affects the fight with FIMI implementation of DSA and other EU instruments in member countries. Implementing **the DSA**[186] introduces a certain level of harmonisation in terms of administrative sanctions and obligations of digital platforms. Member states designate various bodies as DSA coordinators, ranging from media regulators to electronic communications authorities, which are to have the power to impose a penalty of up to 6% of platforms' global turnover for DSA violations (France's ARCOM already has such powers). The role of digital services coordinator includes the relevant authorities of the Member States, which, however, differ in their scope of competence - which also translates into their ability to implement regulations and act in accordance with the DSA, especially in the context of combating FIMI.

Some authorities deal exclusively with telecommunications (e.g. UKE in Poland). Others combine media and telecommunications supervision (e.g. AGCOM in Italy, ARCOM in France). Some also have broader competences covering: competition protection (e.g. CNMC in Spain), consumer protection (e.g. PTAC in Latvia), postal services (e.g. BIPT in Belgium), transport (e.g. TRAFICOM in Finland).

Not all authorities have the same regulatory powers. They can be divided into several categories: Authorities with full regulatory powers in the area of media and content: ARCOM (France) – has specific powers to combat disinformation, can impose penalties on online

[184] Presentation titled "Media Literacy in Practice in Spain and Portugal", Iberifier, November 16, 2022, Cidadania e desinformação (media-and-learning.eu)
[185] *Media Services Act*, https://www.riigiteataja.ee/en/eli/511012019003/consolide
[186] https://digital-strategy.ec.europa.eu/en/policies/dsa-board

platforms[187]; AGCOM (Italy) – has a dedicated disinformation monitoring team[188] and Technical Table[189]; CNAM (Ireland) – oversees the implementation of the Digital Services Act, including disinformation issues. Regulators with partial competence to combat FIMI: CSA (Belgium) – can act in case of disinformation in audiovisual media; CRTA (Cyprus) – limited to traditional media. Differing technical resources and competences of national authorities result in different approaches to DSA enforcement in the area of disinformation and digital services.

In terms of competences related to combating FIMI, there are also important differences between national DSA coordinators. So far, telecommunications authorities (e.g. the Polish UKE, the Swedish PTS) and authorities focused on infrastructure and the protection of competition rules (e.g. the German BNETZA) have not had such competences. Others share these competences with other actors in the co-regulation model recommended by the DSA, e.g. KommAustria and CNMC (Spain) work with digital platforms and fact-checkers and have a clearly defined role in the broader strategy to counter disinformation.

In terms of the scope of content supervision, regulators like the French ARCOM or Italian AGCOM have broad powers of direct intervention, while other bodies like the Polish UKE or Swedish PTS are limited to monitoring and reporting functions. In between these two poles are regulators like the Belgian CSA or the Spanish CNMC, which can make recommendations and have limited intervention powers. Enforcement tools also differ significantly: while ARCOM (France) and CNAM (Ireland) can impose significant financial penalties and demand the immediate removal of content, the competences of other bodies, such as TRAFICOM (Finland) or ANACOM (Portugal), are mainly limited to data collection and analysis. The field of action of regulators also varies, with some bodies, such as Hungary's NMHH or Austria's KommAustria, having comprehensive powers covering both traditional media, online platforms and social media, while others, such as Germany's BNETZA, focus mainly on traditional media and the associated telecommunications infrastructure. These differences in powers, competences and regulatory tools translate into a heterogeneous scope, manner and differences in capacities to intervene in the media space related to countering disinformation.

The competence of regulators is constantly evolving adapting to EU regulations like the DSA/DMA and the changing challenges of disinformation. However, significant differences in the competences and powers of national regulators translate into the way EU regulations are implemented in the area of combating disinformation. ARCOM (France) and CNAM (Ireland) represent a centralised model, where a single authority has broad powers coinciding with the expectations of the DSA, including the ability to impose penalties on digital platforms and respond directly to disinformation incidents. In contrast, the distributed model, seen in the case of Germany's BNETZA or Poland's UKE, is characterised by the division of powers between different institutions, often leading to prolonged decision-making and

---

[187] A. Blocman, *Platform regulation and DSA implementation: ARCOM an European Commission incrase cooperation*, IRIS Legal Observations of the European Audiovisual Observatory, https://merlin.obs.coe.int/article/9903.

[188] The monitoring team work's within Department of Economics and Statistics. https://web.archive.org/web/20200820140058/https://www.agcom.it/documents/10179/18199220/Documento+generico+01-04-2020/47636882-2d30-42dd-945d-ffc6597e685f?version=1.0

[189] *Tavolo tecnico*, which involving broadcasters, digital platforms, academics, etc. https://www.agcom.it/tavolo-tecnico-07-giugno-2024, [accessed: 27.06.2024]. Example of public consultations on regulations regarding removing malicious online videos: https://web.archive.org/web/20230509160315/https://www.agcom.it/documents/10179/29559719/Delibera+22-23-CONS/1e92c9c1-53fb-4229-b92a-ca91613a42d4?version=1.0

potential enforcement gaps. The hybrid model, represented by Spain's CNMC or Italy's AGCOM, combines different competences in a single institution, maintaining flexibility to respond to new challenges. The Belgian system with CSA and IBPT shows how the division of competences can lead to the need for close cooperation between authorities. This differentiation results in an uneven ability to combat disinformation in the EU – while ARCOM can impose significant fines and demand immediate removal of content, regulators like Hungary's NMHH or Slovenia's AKOS have limited ability to intervene directly, despite the common legal framework under the DSA. This implementation heterogeneity does not necessarily undermine the effectiveness of a pan-European strategy against FIMI. National implementations should be monitored and their translation into national capacities to counter FIMI should be evaluated. In the event that national actors clearly differ in their effectiveness in responding to the same types of attacks, any clarification of such incidents translated into further regulation may help strengthen European information resilience.

4.4. Effectiveness of the legal instruments to combat disinformation in EU countries

The implementation of regulations to combat FIMI is still in its early stages. In Latvia, spreading false information can be prosecuted under laws like Article 321 (hooliganism) and Article 157 (defamation). According to the Saufex survey, those regulations are "rather adequate". Article 231 of the Latvian Criminal Law "expressed in obvious disrespect for the public or in dishonesty, ignoring generally accepted behavioural norms," which include activities involved in disseminating knowingly false content or information that hinder the 'peace of the people', institutions, or companies". In 2021, Latvia became the first Baltic State to convict an individual for spreading false information online (about Covid-19 pandemic). The court sentenced him to seven months in prison for hooliganism and incitement to ethnic hatred. In 2024, amendments to Criminal Code introduced criminal liability for influencing elections with deep fake technology, with up to five years of imprisonment for using such technology to spread false information about political parties or candidates. It says that "outlaw the use of manipulated social media accounts to disseminate information aimed at harming the constitutional order, territorial integrity, defense, or other interests of the state" (Article 90).

When analysing the practical effectiveness of legal instruments in the fight against disinformation, it is worth looking at specific Austrian and German cases that have come before law enforcement authorities or courts in recent years. These cases illustrate the variety of forms of disinformation - from personal defamation to false reports of crimes to disinformation related to public health in the context of the COVID-19 pandemic. It is particularly interesting to note that despite the existence of various legal provisions potentially applicable to disinformation cases, in practice it proves difficult to successfully prosecute and convict perpetrators. Most cases end up being discontinued, do not go to trial or cases are settled out of court, for example through settlements or payment of fines. The cases presented below also illustrate the practical challenges of enforcement in the digital environment.

Table 5: Examples of criminal cases for offences akin to disinformation in Austria and Germany

Case	Subject	Legal Basis	Verdict
Ignaz Bearth case (2019)	Facebook post with fake quote attributed to politican about a murder case in Freiburg	§ 188 German Criminal Code (Defamation of persons in political life)	Convicted, fined 90 daily rates of €30

Eva Glawischnig case #1	Facebook post claiming political party demanded "sex with minors from age 12"	§ 111 StGB (Defamation)	German user sentenced to 2 months suspended sentence and €300 compensation
Eva Glawischnig case #2	False health claims about cancer and dementia	§ 264 StGB (Spreading false news during elections)	Complaint filed, no trial mentioned
Innsbruck Police Officer case (2021)	Facebook post with a photo alleging police misconduct at an anti-COVID-19 measures protest	§ 111 StGB (Defamation)	Multiple trials against people who shared the post
Dr. Nashat Kirbaa case	WhatsApp voice message claiming patient deaths and vaccine injuries (COVID-19)	§ 111 StGB (Defamation); § 152 StGB (Kreditschädigung)	Perpetrator identified, further proceedings not known
Kickl v. Rosam case (2021-2023)	Allegations that a prominent anti-vaccine politician received a secret vaccination. (COVID-19)	Civil case for defamation	Kickl lost (courts ruled statement was protected speech)
Michael O. case	Fake quote attributed to Eva Glawischnig about refugees	§ 111 StGB (Defamation)	Acquitted (court considered it legitimate political satire)
Gil Ofarim Case (2021-2023)	False claim of antisemitic discrimination at Leipzig hotel	Defamation and false accusation (German Criminal Code)	Case dismissed after guilty plea and €10,000 fine payment
Duisburg Case (2016)	Blog post about fictional rapes and kidnappings of schoolgirls by refugees	Incitement to hatred (§130 German Criminal Code)	Convicted
Dominik Nepp Case	Statement blaming asylum seekers for rising COVID-19 cases in Vienna, using term "asylum seeker virus"	Incitement to hatred	Charged, no verdict information availible
Lageso Case (Berlin, 2016)	False report about Syrian refugee's death at health and social affairs office	Faking a criminal offense (§145d German Criminal Code) considered	No criminal proceedings initiated
Tennengau Case (Austria)	False report about COVID-19 case in community	Landzwang (§275 Austrian Criminal Code) *Causing fear and distress to the public or to a large group of persons by threatening an attack on life, health, physical integrity, liberty or propert*.	Police report filed, likely unsuccessful due to lack of *threat* element.
Kaiserslautern Case (2020)	False online report about coronavirus case	Faking a common danger	Two perpetrators identified, no verdict information provided
Case against Facebook (Modamani)	False accusations linking Syrian refugee to Berlin Christmas market	Civil case against Facebook for content removal	Injunction request rejected by Würzburg District Court

	attack and other crimes through photo manipulations		

Source: S. Ritter, *„Die Verbreitung von Desinformation im Lichte des österreichischen Strafrechts“*, Master Thesis University of Vienna, Vienna 2024, pp. 40, 66-68, 70-72, 76-77, 105, 114-115, 124-127.

The problem with implementation of does not lie in the lack of appropriate legal tools, but in the fundamental difficulties of proving responsibility for disinformation, identifying perpetrators in the digital environment and the risk that an overly restrictive approach may paradoxically reinforce public distrust and conspiracy theories. The examples from Austrian (the experience with §276 of the Austrian Penal Code[190]), or the problems of enforcing liability of social media platforms, shows the limitations of a legal sanctions approach. Some countries suggest that instead of creating new legal mechanisms, the focus should be on strengthening societies' resilience to disinformation through media education, fostering professional journalism and increasing the transparency of digital platforms. In the context of FIMI, it may be more effective to combine existing legal instruments with diplomatic, technical and educational efforts than to create new regulations.

The cases analysed, such as the false reports of refugee crimes in Duisburg or Treuchtlingen (which were shared more than 100 times in just two hours), or the disinformation concerning COVID-19 in the Tennengau case, represent domestic incidents. However, the way they are spread – through social media, fake profiles, manipulated photos (as in the Modamani case) or viral videos (the Ofarim case) – shows that single incidents of disinformation can easily be used in broader, international influence campaigns (FIMI). In particular, narratives that are anti-immigrant or that undermine trust in the actions of authorities during a pandemic can be amplified and multiplied by external actors to deepen social polarisation and undermine European values. While existing national laws, as shown by cases of successful prosecutions for incitement to hatred or defamation, may be sufficient to counter disinformation coming from perpetrators acting within a country's jurisdiction, they remain powerless against coordinated disinformation campaigns from abroad. This is evidenced, for example, by the limited effectiveness of legal action against social media platforms (the Modamani casus), which are often used as channels for the distribution of disinformation by external actors. This suggests the need to develop new legal mechanisms at the international level to effectively identify sources of disinformation originating from outside the EU and to impose sanctions on its perpetrators.

The effectiveness of enforcement of the adopted regulations also varies – in Italy, according to interviewed expert, so far no one has been indicted for spreading disinformation, and in many countries regulations remain dead. An interesting case is that of Malta, where Article 82 of Malta's Criminal Code forbids spreading false information and provides for a three-month prison sentence for *maliciously spreading false news which is likely to alarm public opinion or disturb public good order*. Some countries, such as Portugal, have taken a more general approach – the Charter on Human Rights in the Digital Age defines disinformation as *any narrative that is demonstrably false or misleading created, presented and disseminated for economic advantage or to deliberately mislead the public*, but these provisions have not yet translated into criminal regulation.

[190] §276 of the Austrian Criminal Code (repealed in 2015) - a provision criminalising the *dissemination of false and disturbing rumours*, has not led to any conviction in 20 years. Sabina Ritter used this case as an argument against the creation of dedicated criminal laws to combat disinformation due to their practical ineffectiveness while risking excessive interference with freedom of expression. S. Ritter, *„Die Verbreitung von Desinformation im Lichte des österreichischen Strafrechts“*, Master Thesis University of Vienna, Vienna 2024, pp. 128, 141, 145-147.

In terms of regulatory trends, an increase in the importance of deepfake legislation is evident, as evidenced by the example of Latvia, where criminal liability for influencing elections with deep fake technology, with up to five years of imprisonment, was introduced in 2024. Increased attention is also being paid to the protection of electoral processes, as reflected in French legislation e.g. Law no. 2018-1202 which aims to protect democracy against false information that could distort the integrity of a vote.

The diversity of regulatory approaches reflects differences in priorities, legal traditions, geopolitical contexts and perceptions of disinformation threats among EU Member States. At the same time, the common legal framework being developed at EU level, particularly in the form of the DSA, aims to develop a more unified approach to combating disinformation in the digital space. From this, there is a clear variation in the approach of the Member States to the regulation of countering disinformation. The analysis allows the identification of several distinctive models of regulatory interference.

4.5. Conclusions

The EU addresses FIMI through a broad mix of administrative, civil and criminal laws, and aimed at regulating information content. No EU member state has specific legislation directly targeting FIMI, so the issue is generally managed through indirect regulations on media, internet activities, and advertising. Although constitutional protections for freedom of expression and the right to information exist, they are not very effective in combating disinformation due to the lack of legal instruments for practical enforcement and inadequacy in the face of modern realities.

The EU's broad legal tools against disinformation include laws on defamation, incitement to hatred, and hooliganism, among others. Individual EU countries are taking different approaches: in Latvia, laws on hooliganism and defamation have been used to prosecute disinformation, with recent amendments penalising the use of deepfake technology to influence elections. Estonia's legal framework targets disinformation that endangers public health. Poland recently introduced legislation with severe penalties for disinformation linked to foreign intelligence. In contrast, Hungary lacks binding regulations due to limited political will, relying instead on non-binding recommendations, which have proven ineffective.

The constitutional provisions on freedom of expression and the right to information are not very effective in combating disinformation due to the lack of legal instruments to support the practical implementation of these provisions and the inadequacy in the face of modern realities.

Various types of regulation across EU countries are aimed at directly targeting information manipulation. States define the need to combat FIMI differently, addressing concerns such as public order, national security, individual or institutional reputation, constitutional order, sovereignty, territorial integrity, defence capabilities, economic stability, public health, and personal rights affecting human dignity. Overall, EU efforts to counteract FIMI are still in early stages, with diverse national approaches reflecting different priorities for protecting public order, security, and institutional integrity. These varied approaches reflect each country's priorities in safeguarding public interests against FIMI.

The geopolitical context emerges as a crucial determinant in shaping national approaches to disinformation regulation, with a clear East-West divide in regulatory intensity. The Baltic states and Poland demonstrate the most stringent regulatory frameworks, directly influenced by their proximity to Russia and historical experiences. This is evidenced in Lithuania's 2017

security strategy, which explicitly identified Russia as the primary threat to information security, and Latvia's decisive action in banning Russian TV channels following the invasion of Ukraine[191]. Poland similarly responded with immediate measures, including the removal of Russian propaganda channels through KRRiT resolution in February 2022.

The influence of **legal traditions** and **EU membership** emerges as another crucial factor in shaping national approaches to disinformation regulation. A distinct pattern can be observed where some member states, exemplified by Luxembourg, deliberately refrain from developing national legislation, preferring to await comprehensive EU frameworks. This wait-and-see approach contrasts with the proactive stance taken by other member states. Romania's swift adoption of Law No. 50/2024 in March 2024 demonstrates this commitment to harmonizing national legislation with EU requirements, while Bulgaria's implementation of the DSA has already catalyzed significant changes in their legal framework and institutional infrastructure, particularly in the areas of user protection and platform accountability. This varying pace and approach to EU regulatory alignment reflects broader differences in legal cultures and institutional capacities across member states, with some countries viewing EU frameworks as an opportunity to modernize their digital governance structures, while others prefer to maintain regulatory flexibility until EU standards are fully established.

The variation in **political culture and media traditions** across EU member states shapes their approach to disinformation regulation. Sweden exemplifies a strong democratic tradition where freedom of expression is constitutionally enshrined as a paramount right, with explicit legal presumption favoring free speech over other competing interests. This approach starkly contrasts with the situation in countries like Hungary, where a lack of political will to counter disinformation has resulted in minimal effective regulation, relying primarily on non-binding recommendations that SAUFEX survey respondents characterize as ***highly ineffective***. These divergent approaches reflect deeper differences in democratic traditions and institutional trust across the EU. In countries with strong democratic institutions and high trust in media self-regulation, the emphasis tends to be on preserving press freedom while addressing disinformation through media literacy and voluntary compliance mechanisms. Conversely, in states with different historical experiences and institutional frameworks, the balance between media freedom and state oversight often tilts toward more direct government intervention, though not always resulting in effective countermeasures against disinformation.Analysis of current trends in EU member states' approaches to disinformation reveals several significant patterns and emerging challenges. A clear trend toward increased regulation is evident, with countries like Poland, Lithuania, Cyprus, and Latvia introducing new legislative measures, particularly accelerated by the implementation of the DSA. However, the approaches vary considerably in their comprehensiveness and institutional structure. France exemplifies a centralized, comprehensive approach with its dedicated VIGINUM, while Austria maintains a more distributed framework, utilizing existing legal mechanisms to address various aspects of disinformation. These divergent approaches have highlighted critical challenges, particularly in balancing security concerns with freedom of expression. Poland's experience with the Draft Law on the Protection of Freedom of Expression on the Internet illustrates this tension, with the Ombudsman warning against potential restrictions on free speech through arbitrary state decisions. Institutional independence also emerges as a significant concern, as evidenced by Romania's controversy over the appointment of ANCOM's president, raising questions about

[191] Decision based on Electronic Mass Media Law article 26, that prohibits i.a. „calls for war". *Elektronisko plašsaziņas līdzekļu likums*, Latvijas Vēstnesis, 118, 28 July 2010, https://likumi.lv/ta/id/214039-elektronisko-plassazinas-lidzeklu-likums

regulatory body autonomy. The Russian invasion of Ukraine has served as a catalyst for enhanced state authority in combating disinformation, particularly in Central European countries, yet the varying approaches among member states continue to reflect their distinct historical contexts, geopolitical positions, and legal cultures. This diversity in regulatory responses, while demonstrating the complexity of addressing disinformation, also underscores the ongoing challenge of developing effective countermeasures while preserving democratic values and institutional integrity.

An analysis of the legal regulation of disinformation in EU countries reveals a significant diversity of legislative approaches. Most EU Member States do not have dedicated criminal legislation directly addressing the phenomenon of disinformation. Regulations are most often part of a broader legal framework, including media law, electoral law or cyber security legislation.

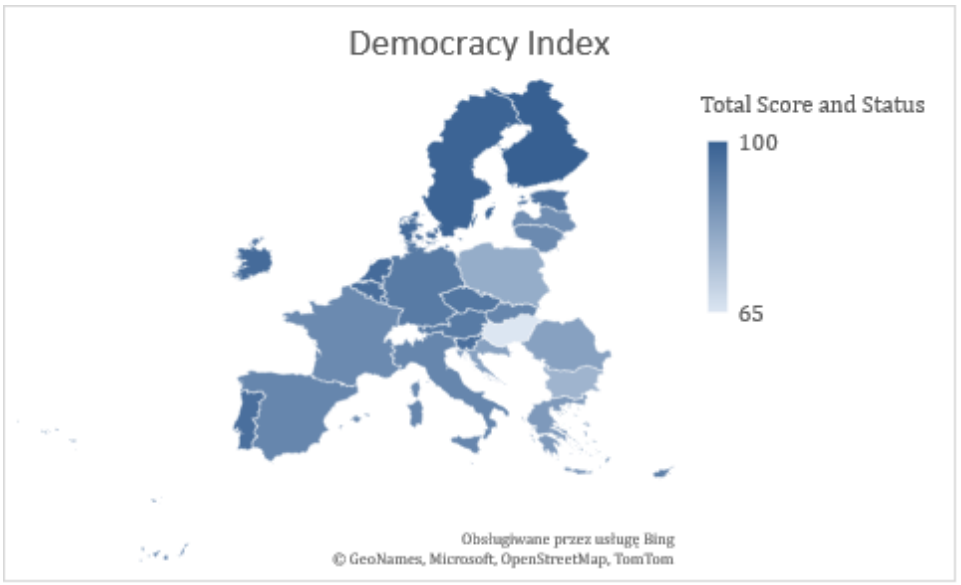
Part V – SOCIETAL RESILIENCE

Katarzyna Golik, Sara Nowacka

5.1. Democracy and Societal Resilience

Societal resilience refers to the ability of a community to withstand, adapt to, and recover from challenges, including disinformation campaigns and social unrest. The capacity for resilience is often augmented by social cohesion, which fosters trust and collaboration among community members. Meanwhile, media literacy equips individuals with the skills to critically assess information, enabling them to discern fact from falsehood. Together, these elements create a robust foundation for societal resilience, particularly in contexts where misinformation proliferates.

This section seeks to map out the state of democracy among the EU countries within the context of societal resilience against FIMI. Although FIMI, by the definition, is a tool used by foreign powers against another country, it thrives on internal disputes and domestic political instability. Both, the desk research and the survey proved that foreign interference was using social controversies and moot points as fundamentals for spreading disinformation and was built on current events which had a potential to create cracks in the society's cohesion or deepen the ones already present.



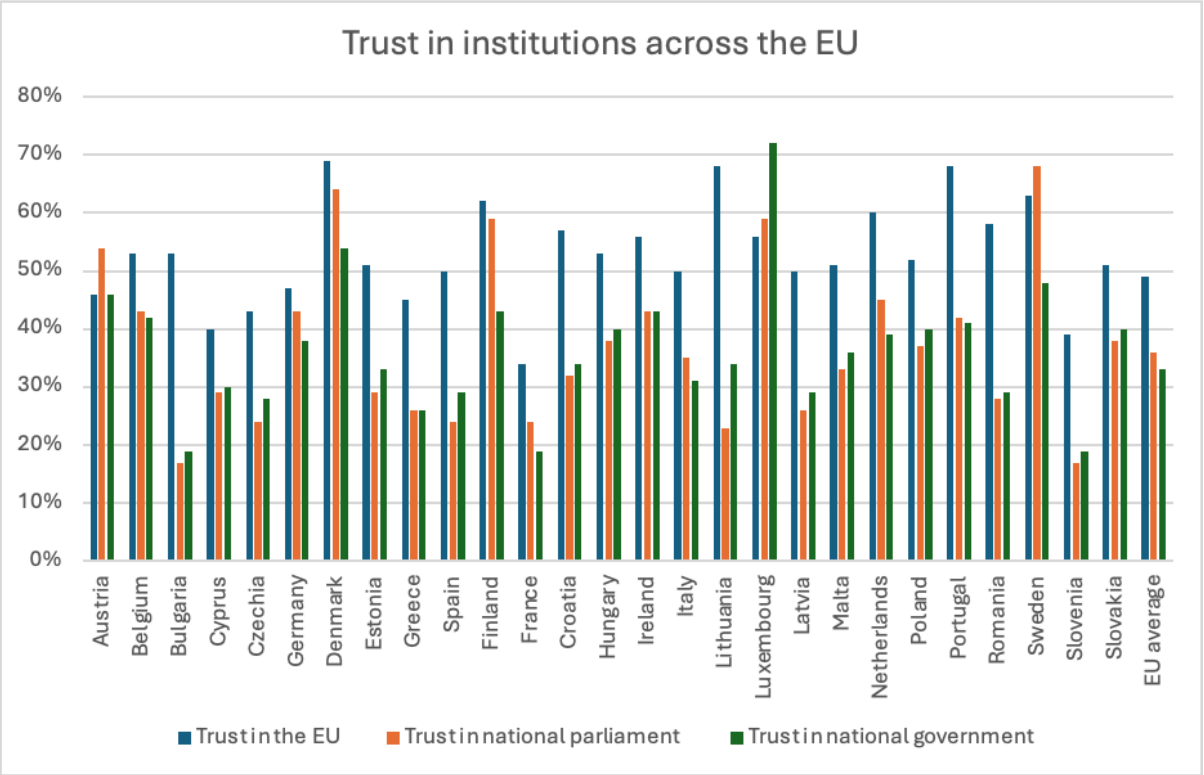
Source: Based on Freedom House data.

EU states vary widely in their internal stability and thus in the levels it influences their resilience to FIMI. It is influenced by local political landscapes, media independence, and societal cohesion. The effectiveness of countermeasures and debunking efforts often hinges on state-media relationships and media funding, with cross-sector collaboration proving crucial and often a decisive factor in the most resilient states.

At the same time, there is also an opposite vector interaction – social coherence, trust for the government, cross-sectoral collaboration and ability to resolve internal disputes without them causing a significant opportunity for threat actors is also strengthened by strong regulation and institutions guaranteeing media freedom and independence. Therefore, the relationship between social coherence/internal stability and strong, effective regulation regarding FIMI is best described as circular, where one element is directly affecting the condition of another.

Hence, the context of FIMI and disinformation vulnerability highlights the essential character of robust democratic practices for a stable and resilient society. European states that embody these democratic strengths tend to have lower FIMI susceptibility. They maintain stable institutional and social structures through transparent governance, independent media, cohesive social policies, and high media literacy, enabling a comprehensive defence against manipulation. Democratic strength, in this context, is less about form and more about the depth of democratic engagement across media, civil society, and governance—forming a multi-layered defence that empowers citizens to recognize and counter disinformation. Within this context three variables were distinguished as those influencing societal response to FIMI.

5.1.1. Trust in Democratic Institutions



In strong democracies, citizens generally trust their institutions, which include transparent governance, an accountable judiciary, and a responsive government. This foundational trust helps immunize societies against FIMI tactics that aim to exploit cynicism, disenchantment, or apathy towards democratic structures.

The cases of Bulgaria and Romania highlighted that low trust in state institutions is corelated with their weakness which tends to be exploited be threat actors for spreading disinformation. This weakness hampers possibilities for cross-sectoral cooperation and decrease legitimacy of state-led counter disinformation efforts aimed i.e. at strengthening media literacy.

On the other hand, Denmark seems to be important case in point, where exponentially high trust for public institutions goes in pair with strong conviction that citizens in their country can access accurate information from multiple media sources, which is strengthened by government involvement in awareness rising initiatives.

5.1.2. Levels of Political and Social Polarization

Threat actors take advantage of pre-existing conflicts or current affairs bearing a potential to cause or deepen cracks within the social cohesion of a given state. Societies with lower levels

of polarization are generally more resilient to divisive narratives propagated through disinformation. Strong democracies often engage in consensus-driven politics, reducing the appeal of extreme ideologies and limiting FIMI's effectiveness in sowing division.

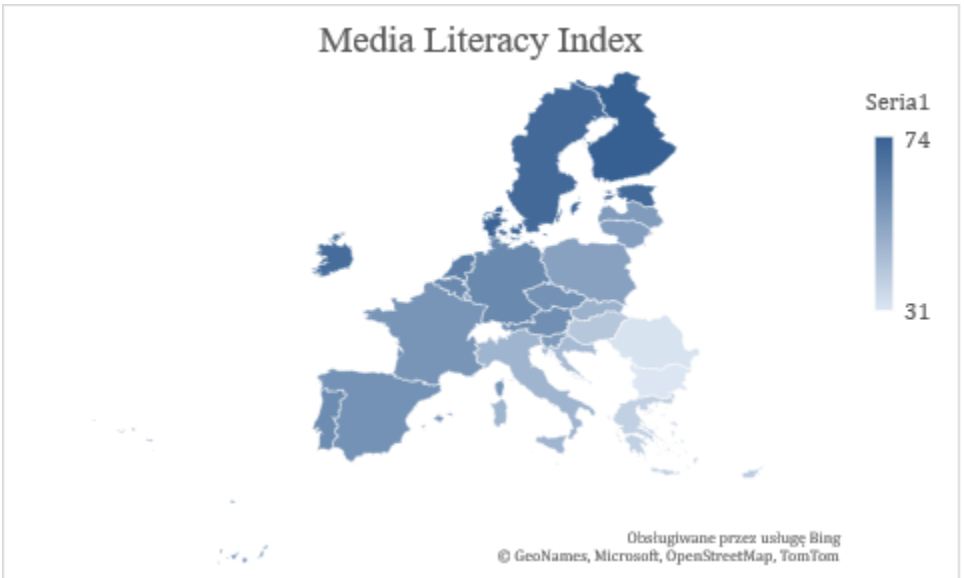
Finland demonstrates resilience to polarization, partly because of institutional setups that prioritize representation across diverse communities. In Portugal, relatively young democracy and belief that democratization brought about a positive change decreases potential for polarizations while at the same time increasing societal resilience.

In Belgium on the other hand, fragmentation around linguistic communities prevents strong national initiatives from emerging. Similarly, in Spain, where local identities can resonate stronger than the national ones, pro-independence or separatist aspirations can become platforms for threat actors to spread content which favors their interest. In Bulgaria a long history of connections to Russia fuels polarization and divisions related to Russia/Ukraine war, while in Romania growing social polarization, nationalism, populism and social conservatism challenging Western liberal values, as well as high levels of corruption enhances social vulnerability. In Poland it was also noted that high levels of polarization provides for significant point of departure for Russian disinformation, despite the normally high resilience of Polish society against manipulation by this particular actor.

5.1.3. Media Landscape and Transparency

A strong democracy supports an independent, diverse media landscape free from excessive political or economic influence. Such a media environment allows citizens access to balanced information and provides checks on misinformation, as pluralism in media reduces the dominance of any single narrative or bias. Positive impact of media-driven initiatives focused on factchecking is mirrored by cases of Spain, where organizations such as Maltida.es or Iberifier focus on grass-root approach to debunking or Lithuania where the biggest news portal delfi.lt has developed a tool to combat "fake news" in cooperation with Google.

At the same time, however, the media in countries such as Hungary, Bulgaria, Romania or Cyprus face political pressure. In these countries major outlets tend to be financed by political parties (Romania), influenced by business or church (Cyprus), lack of funding regulations (Bulgaria) or political pressure and governmental monitoring through surveillance tools (Hungary).



Source: Based on Open Society Institute Sofia data.

Hence, this sector requires stable work conditions as well as independent and sustainable funding, especially for traditional media outlets and factcheckers. The cases of Ireland, Denmark and Latvia highlighted that work conditions and financial constraints influence the extent to which the media can protect itself and citizens from FIMI and disinformation. Study pointed to the layoffs and financial problems faced by Irish broadcasters and unstable media funding in Latvia and Denmark.

Source: Based on Reporters sans frontieres data.

These three variables allowed to group EU states accordingly:

Group 1: High Strength in Democratic Characteristics

These states have high institutional trust, independent media, robust media literacy programs, active civil society, and low polarization, making them resilient to FIMI.

Countries: **Finland, Ireland, Netherlands, Denmark, Sweden, Luxembourg**

Characteristics:

- **High public trust in institutions** and **effective collaboration** between the government and NGOs on disinformation efforts.
- **Independent media landscapes** with strong freedom of the press and high media trust.
- **Advanced media literacy education** programs integrated into the educational systems, particularly in Finland and Denmark.

Examples: Finland's comprehensive media literacy initiatives and strong civic engagement, alongside Ireland's Media Literacy Ireland network and collaboration on fact-checking, underscore these countries' resilience. Also, the support of the Danish government for media, driven largely by a political will to support and uphold media in Danish language and media plurality, positively impacts its potential for fighting FIMI. Such initiatives are transparent and fair for both state and private media. This helped Denmark avoid issues with politically affiliated business owners controlling major media outlets for political influence unlike other countries in the EU.

Group 2: Moderate to High Strength in Democratic Characteristics

Countries in this group exhibit generally high democratic characteristics but may have specific vulnerabilities, such as moderate polarization or challenges with media independence.

Countries: **Germany, Austria, Belgium, Estonia, Lithuania, Portugal, Slovenia**

Characteristics:

- **Generally strong institutional trust** and **active civil society organizations** that work on disinformation countermeasures.
- **Moderate media independence** with a strong public broadcasting system, though some countries face challenges in funding independent media.
- **Good media literacy programs**, with varying degrees of effectiveness.

Examples: Germany's Correctiv initiative reflects a robust civil society effort to counter disinformation, while Belgium's EDMO BELUX collaboration illustrates active state-civil cooperation. The Austrian approach to FIMI is balancing the need to protect against disinformation with respect for fundamental rights, including freedom of expression and the arts. Austria prefers to educate and promote awareness of the dangers of disinformation, rather than to introduce additional legislation. This is evident in the "Deepfake Action Plan" and other above-mentioned documents, that emphasizes building social resilience, strengthening digital competences and promoting reliable information sources.

Group 3: Moderate Strength with Notable Vulnerabilities

These states show moderate strength in democratic attributes but face issues with either polarization, lower media trust, or civil society's limited influence, which leaves them more vulnerable to FIMI.

Countries: **France, Spain, Czech Republic, Latvia, Italy, Poland, Croatia**

Characteristics:

- **Mixed institutional trust** and **moderate media literacy** levels, often with active but regionally varied civil society engagement.
- Some challenges with **polarization and social divides**, such as in France and Spain, where regional tensions can be exploited by disinformation.

Examples: Spain's regional polarization (e.g., Catalonia) provides an entry point for external narratives, while France's media efforts, such as AFP Factuel, show resilience tempered by lower institutional trust (only 19% French respondents trust their national government). In Spain regional separatist movements, especially in Catalonia, facilitated widespread disinformation campaigns and social fragmentation. This vulnerability was worsened by complex interactions between local autonomy and state intervention, creating fertile ground for external actors to exploit divisions. Russia used the illegal independence referendum organized in 2017 and the institutional crisis that followed as a vehicle for spreading disinformation, which highlighted the opportunistic character of FIMI. Russian officials reportedly maintained contacts with members of the Catalan independence movement during the referendum period. It was part of a broader effort to cultivate and support separatist sentiments, which served Russia's interest in creating divisions within EU states.

Group 4: Lower Democratic Strength with High Vulnerability

These states face significant challenges, including high polarization, limited media independence, and lower civil society influence, making them more susceptible to disinformation and FIMI.

Countries: **Hungary, Bulgaria, Romania, Malta, Greece, Cyprus**

Characteristics:

- **Low trust in institutions** and **government-influenced media landscapes**, particularly in Hungary, where media is highly centralized.
- **Limited civil society engagement**, with independent NGOs facing restrictions (as in Hungary's Sovereignty Protection Act).
- **High polarization** and social divides that external actors can exploit, particularly in Bulgaria and Romania.

Examples: Hungary's government-controlled media and Bulgaria's strong Russian influence show how democratic weaknesses heightened susceptibility to FIMI. Russia has capitalized on Hungary's internal political landscape, particularly government-controlled media and political polarization, to spread disinformation and promote narratives sympathetic to Russian interests. Hungary's media landscape is dominated by entities that support the ruling Fidesz party, which frequently promotes narratives in line with Russian perspectives. This alignment gives Russian narratives an open channel through which they can reach the Hungarian public without strong opposition, effectively blending Hungarian and Russian agendas in the media space. Hungary's Sovereignty Protection Act exemplifies state-led media control, targeting NGOs and independent media with foreign funding, mirroring Russian tactics. The act reveals how Hungary's approach to media and NGO regulation enhances domestic disinformation vulnerabilities.

Source: Based on European Quality of Government Survey (EQI) Index data on Confidence in Parliament and Elections' Fairness.

5.2. Variety of Connections to Russia

In this subchapter we look into historical and present connections to potential threat actors (Russia, China, other autocratic states) and try to analyze to what extent they facilitate FIMI operations.

Some states developed various types of links with Russia, which created positive sentiment among segments of society. These factors can include business contacts, penetration by the Russian capital, as well as historical or religious links via Eastern rites of Christianity. Significant examples include Cyprus, Bulgaria, or Baltic states. The financial and political influence of Russia and other foreign actors is a source of vulnerability for Cyprus to disinformation campaigns and foreign interference. Many Cypriot politicians and influential figures acted in Russia's interests, to the detriment of their own country and the EU, as evidenced by the 2023 “Cyprus Confidential” study by the International Consortium of Investigative Journalists. One of the reasons behind that is the role of tax safe haven that Cyrpus plays for many Russian oligarchs.

Bulgaria, on the other hand, is exposed to increased Russian influence through the heavy dependence of its energy sector on Russian resources and the Kremlin's significant cultural capital in Bulgaria, which translates not only into public sentiment but also indirectly into the workforce in state sectors such as special services, diplomacy and judiciary. A tangible example is the high degree of infiltration of Bulgarian institutions by the Russian intelligence apparatus. Allegations of espionage were even brought against the employees of the Chief Directorate for Combating Organised Crime and State Agency for National Security, institutions involved in countering FIMI.

In Estonia around 27% of the population is Russian speaking. It is reported that it is the most difficult to integrate into Estonian society. Following the full-scale Russian invasion, according to the research by the Fredrich Ebert Foundation, 50% of the Russian-speaking minority agreed with the statement that Russia had a right to use military force against Ukraine to prevent it from joining NATO, while among Estonian-speaking families only 1% of citizens supported this statement. Latvia and Lithuania face a similar challenge with Russian-speakers constituting 25-30% and 16% of the whole population respectively.

5.3. A Patchwork of NGOs Relations with Society, Media and Governments

The interplay between social cohesion and media literacy emerges as a cornerstone of societal resilience, particularly in fragmented and polarized environments. An effective approach involves the collaboration of non-governmental organizations (NGOs) with governmental bodies, the media, and civil society. While instances of cooperation have been documented in various countries, challenges such as conflicting interests and tensions often complicate these relationships. In some cases, even when proactive media literacy initiatives and fact-checking programs exist but are sometimes perceived as ineffective, underscoring the need for a more cohesive strategy. A well-developed NGO sector, complemented by educational outreach that promotes media literacy, plays a pivotal role in fostering trust and resilience in society. In advanced economies, where democratic values are entrenched, the framework for these collaborations tends to be more robust. However, the sustainability of such initiatives requires an ongoing commitment to fostering trust and transparency among all stakeholders.

5.3.1. Fact-checking Initiatives and Media Literacy Education

NGOs play a pivotal role in enhancing social cohesion and media literacy. Various case studies across Europe reveal that cooperation among NGOs, public institutions, and media can yield positive outcomes. The presence of well-developed NGO networks that engage in fact-checking and media literacy education serves as a foundation for building societal resilience. There is a noticeable correlation between the activities of these organizations and the overall trust within society. For instance, France's Agence France Presse (AFP) has established a global network of fact-checkers that actively monitor misinformation. To date, AFP Factuel has more than 140 fact-checkers in 5 continents, covering over 30 countries and 24 languages. They are in constant interaction with other journalists in the AFP network. AFP Factuel is member of the International Fact-Checking Network (IFCN) in France and other members. Despite their efforts, the effectiveness of such initiatives has been not evident, indicating that challenges persist in building societal resilience to FIMI. Similarly, Belgium's EDMO BELUX initiative fosters collaboration among fact-checkers and media literacy organizations to combat misinformation, directly empowering citizens to discern truth from falsehood. In Germany, a comprehensive approach to media literacy has been adopted, supported by government initiatives and independent organizations. The Federal Agency for Civic Education offers resources to enhance critical thinking and media skills among citizens. Moreover, NGOs such as Correctiv and Forum against Fakes maintain independence while contributing to fact-checking efforts. This collaboration between NGOs and governmental bodies exemplifies a model of resilience founded on mutual support and shared goals.

In Netherlands a regional hub from the European Digital Media Observatory initiative Benedmo focuses specifically on the Dutch-speaking community in Belgium and on the Netherlands. It notably documented specific cross-border disinformation campaigns on health and the impact of fact-checking. deCheckers is a non-profit organisation working in partnership with Dutch-speaking fact-checkers. It gathers fact-check articles from various media in a single place. It allows the public to access this information in one portal instead of searching for debunks on multiple websites.

Media literacy emerges as a vital tool in combating misinformation and fostering societal resilience. It equips individuals with skills to critically evaluate information, recognize biases, and distinguish between fact and opinion. Educational programs, supported by governmental initiatives and civil society organizations, play a crucial role in this endeavor.

The effectiveness of media literacy initiatives varies considerably across European nations. For example, Belgium's EDMO BELUX initiative exemplifies a successful cross-community collaboration aimed at combating disinformation. By bringing together fact-checkers, media experts, and academics, EDMO BELUX raises awareness through targeted campaigns and educational programs. Despite this, the overall resilience of Belgian society to FIMI remains "rather low," highlighting that even well-coordinated efforts are not always sufficient to mitigate the threats posed by misinformation.

In contrast, Finland showcases a strong tradition of media literacy that has embedded itself within the educational system. The Finnish National Agency for Education has made media literacy a civic skill, promoting it from early childhood through to vocational training. This proactive stance has yielded high trust levels in news media and a resilient society that is well-equipped to navigate the complexities of the information landscape. Finland's approach underscores the importance of integrating media literacy into the fabric of education and civil society. The German government actively supports initiatives to strengthen public resilience

to disinformation. A key role is played by the Federal Agency for Civic Education (*Bundeszentrale für politische Bildung*, BPB), which offers a wide range of educational materials and programmes on media literacy and critical thinking. The following should also be highlighted: media literacy initiative supported by the Ministry of Interior, and BC4D – media literacy initiative in cooperation with private sector.

The Irish have established a Media Literacy Ireland network, which is an informal alliance of over 250 members who work to promote media literacy in Ireland. Facilitated by Coimisiún na Meán, MLI has over 250 members drawn from a broad range of sectors. The network consists of a broad range of sectors including media, education, NGOs, and libraries. Digital literacy is highly present in the national curriculum in schools, whereas media literacy is only somewhat present and challenges persist in formalising media literacy within national policies and teacher training programmes. Ireland has also multiple grass-root level networks to enhance media literacy in the country.

Numerous Civil Society Organizations (CSOs) in Estonia play an important role in countering FIMI. They work on various fronts, including fact-checking, media literacy education, and public awareness campaigns. For instance, Estonia established the Cyber Defence League, a group of volunteer IT specialists dedicated to sharing information about threats, and cyber security and engaging people in international cyber defense activities. In 2008 Estonia set up NATO's Cooperative Cyber Defence Center of Excellence in Tallinn, which researches FIMI, best practices in cyber defense, and training for NATO members. Another example of a non-state actor is the National Centre for Defence & Security Awareness (NCDSA), established in 2011. The NCDSA is an Estonian non-governmental expert platform dedicated to strengthening national resilience through applied research, strategic communication, and social interaction. The NCDSA runs the state-supported training programme, Sinu Riigi Kaitse, which aims to inform Russian-speaking communities about Estonian national defence and security by initiating and organising public events. Additionally, the NCDSA monitors and analyses the security and defence perceptions of Russian-speakers in Estonia. In Latvia efforts against FIMI are being made together with partners, especially other Baltic states and like-minded countries, through cross-border cooperation at the non-governmental level. For example, the foundation "RE: BALTICA", since August 2011 has been producing investigative journalism and publishing reports on disinformation efforts in the Baltic states, including on social media (an ever-growing hotbed of disinformation).

5.4. Complex Cases - Fragmentation and Polarization

Despite these positive examples, challenges persist. In several instances, tensions and conflicts arise between NGOs and state actors, undermining efforts toward cooperation. In fragmented societies, where divisions based on ideology, ethnicity, or socioeconomic status deepen, it becomes challenging to implement cohesive strategies that address the threats posed by disinformation. In countries where media literacy is not prioritized, such as Italy, societal resilience is significantly undermined, as evidenced by low levels of trust in the media and the prevalence of disinformation. In addition to educational initiatives, the cooperation between NGOs and media organizations is essential for fostering a culture of fact-checking and accountability. Collaborative platforms that engage citizens in identifying and reporting misinformation create a community-oriented approach to combating disinformation. For instance, initiatives like "Maldita.es" in Spain and "Poligrafo" in Portugal mobilize public participation in fact-checking processes, empowering citizens to challenge false narratives actively. Such grassroots efforts not only enhance media literacy but also strengthen cohesion by fostering a sense of shared responsibility towards combating misinformation. Nonetheless, the effectiveness of these initiatives is often contingent upon the

broader political and social landscape. In countries with high levels of corruption or political polarization, such as Romania and Bulgaria, societal resilience is severely compromised. The public's distrust in state institutions and the media diminishes the impact of educational efforts and grassroots initiatives aimed at enhancing media literacy. In such contexts, fostering social cohesion becomes increasingly critical, as it serves as a counterbalance to the divisive forces perpetuated by disinformation campaigns.

In Czechia in 2018, experts from the European Values Center produced a Prague manual for countering Russian influence operations in Europe. The country has traditionally featured a strong civil society (e.g. Czech Elves, European Values Center and Manipulátoři). The *elves* (active members of the society) in the Czech Republic, inspired by examples from the Baltic States, track accounts and onlin platforms, catching other related activities such as actions of spreading disinformation emails about Covid-19. The Czech Demagogue became an inspiration for Polish fact-checkers. The biggest achievement of the Czech non-governmental sector in countering disinformation is the development of the 'the Conspiracy Atlas' – a web-based database of conspiracy theories, populist framing and misinformation from the online world.

The landscape of societal resilience is far from uniform. In several countries, including Poland and Hungary, the interplay between governmental entities and NGOs presents complications. In Poland, public trust in state institutions is low, resulting in a fragmented approach to combating disinformation. In the first half of 2022, eleven NGOs and research institutes jointly developed the 'Code of Good Practice – Together Against Disinformation'. While NGOs have become increasingly aware of foreign influence operations, their initiatives often lack the necessary support from government institutions, leading to what experts describe as cognitive capture—where public institutions between year 2016-2023 adopted anti-Western narratives due to political polarization. This fragmentation hinders effective cooperation and diminishes the potential impact of media literacy and cohesion initiatives. The low level of trust among citizens in governmental institutions exacerbates the issue, resulting in a society vulnerable to disinformation. Poland's weaknesses were identified as the selectivity of actions in cyber-security, dispersion of competences at the administrative levels, and neglect in education and support for independent media. In case of Poland, high awareness of the threats posed by disinformation exists primarily among state institutions and NGOs, but not whole society what needs to be improved. One of Polish weaknesses was lack cooperation between administration and NGOs. In recent years, a number of initiatives have emerged in Poland to combat disinformation (eg. InfoOps, DisinfoDigest, PAP Fake Hunter, Pravda), fact-checking (eg. Demagog) or media education (eg. Panoptykon, Fundacja Nowoczesna Polska). Representatives of the civil society also highlighted a need to devise a national information security strategy. In the first half of 2022, eleven NGOs and research institutes jointly developed the 'Code of Good Practice – Together Against Disinformation'. The code attempts to standardise standards in the fight against disinformation. The experts co-authoring the report have included key issues in this area of information security.

Hungary presents a particularly stark example of how state-NGO relations can deteriorate. The political climate has increasingly restricted the activities of NGOs, resulting in a media landscape that is dominated by pro-government narratives. The Hungarian government's tactics, including the enactment of the Sovereignty Protection Act, have systematically undermined independent journalism and stifled dissent. In this context, the potential for NGOs to foster social cohesion and enhance media literacy is severely limited, leading to dangerously low levels of societal resilience against FIMI. Moreover the level of cooperation between state institutions and non-state actors is very low. Not only these two spheres remain completely disconnected, but furthermore, the government is actively trying to limit the

capacity of NGOs. This manifests itself in hiding and restricting access to information for independent journalists. Fees for accessing public relevant information are being increased and state institutions have a significantly extended timeframe for providing it. Representatives of public institutions are not only reluctant, but are even forbidden to talk to journalists. Another materialisation of this approach is the Sovereignty Protection Act adopted in November 2023. The purpose of this law is not entirely clear, but it targets independent institutions (NGO's and Media), drawing funding from foreign (Western) sources. The above approach is based on the Russian model - classifying Western soft power like a threat and the Foreign Agents Act. Hungary have arbitrarily monitored journalists using the anti-terrorist Pegasus software. According to survey respondents the only types of institutions which are actively engaged are: EU institutions; Non-governmental organisations (NGOs); Media and journalists' associations and they are neither effective nor ineffective. There are some independent organisations, which aim to strengthen societal resilience in Hungary including fact-checking initiatives and initiatives aimed at identifying domestic and foreign information manipulation. One of them is the Hungarian Digital Media Observatory (HDMO), a regional hub and part of the European Digital Media Observatory (EDMO), established by a decision of the European Commission. It is a consortium of several organisations: Lakmusz and AFP for the fact-checking sector, Political Capital and Mertek Media Monitor for research and policymaking and Idea Foundation for training activities. The initiatives are rather dispersed and depend on what institutions (mainly foreign ones) are funding. The biggest donors include the German Marshall Fund, the International Republican Institute, as well as like minded embassies (eg. Scandinavian countries and US).

Lithuania had an unsustainable media landscape, dependant on the interest or business groups. Other problems include corruption and discrimination of national minorities, which creates polarization and vulnerabilities. However, the cooperation between NGOs like Debunk, government and active civil society (communities of *elves*) creates quick FIMI response network.

In the Balkan region NGOs actively cooperate among each other, as well as with EU institutions and with local media. Media literacy, including anti-FIMI, training is provided jointly by the NGOs and media associations. The post-Yugoslavian NGOs held an annual security conference in Bled with a FIMI-related topic. They operate in very polarized and ethnically complex environment, often with low or even hostile attitude from the public bodies. Therefore, the NGOs seek for partners abroad, including the EU institutions.

Croatia and Slovenia are a part of the fact-checking network of 6 organizations from 5 countries in the Western Balkan region, represented by the Association for the Informed Public with a platform Faktograf.hr and Ostro.si with a platform Razkrinkavanje.si. Croatian model of building a system for fact-checking in the public domain was well evaluated by the European Commission, which indicates an existing system, not just individual projects or institutions. That suggests Croatia is heading to create an anti-FIMI systemic resilience. On the contrary, what is emphasised in the study by the state agency, Agency for Electronic Media, is a problem in cohesion between the State institutions and society. What is import, AEM provides funds for the NGOs. Other State institution, the Ministry of Culture and Media was accused of trying to censor the journalists with its law proposals. Aditionally, the right-wing portals and bloggers attacked the leading and internationally recognised anti-FIMI NGO, Faktograf, which was closely correlated in time with millions of hacker's attacks and death threats towards the organisation.

Civil society in Slovenia is actively cooperating with other states and under ECAS' international framework including the campaign "Understanding Populism". The Slovenian

partner for that project was InePA. Some studies suggest relatively high resilience of the society against FIMI.

In Malta media and other organisations highlight a highly polarised environment, strongly influenced by political parties. One of the most polarising issues is corruption. The most important bottom-up initiative tackling disinformation is MEDMO. A network of fact-checkers and experts on FIMI and communication who cover these issues in Malta, Greece and Cyprus. The organisation is part of the wider EU-level initiative called EDMO (European Digital Media Observatory).

Greece is a part of the fact-checking communities, like the steering group for the OECD's DIS / MIS Resource Hub, International Centre for Investigative Journalism, Journalism Trust Initiative (JTI) and the Mediterranean hub of the European Digital Media Observatory. Under the Civic Information Office functions platform MediaWatch, there are also Voutliwatch and Ekspizo.gr. From NGOs, activity is shown by the Ellenika Hoaxes funded by Meta, which was however under accusations of FIMI-spreading from the public institutions on the basis of regulation (allowing punishing FIMI-type offenders with significant fines or even imprisonment of up to 5 years, while the media might lose funds from the state withdrawing its commercials). The journalist unions and NGOs internationally and domestically raised protests perceiving it as a limitation of press freedom, mainly by the extended definition of "false information".

Cyprus ranked 65 out of 180 countries in the 2024 World Press Freedom Index of Reporters without Borders (RSF) – just after Sierra Leone and before Argentina, i.e. under the label of "problematic". The RSF's evaluation held that "although freedom of press is guaranteed by the constitution, the government, the Orthodox Church and business interests have significant influence over the media in Cyprus." The unresolved Northern Cyprus question leaves the island state open to influence campaigns. The lack of funds for independent media and adequate salaries for journalists hinder media pluralism and resilience efforts of the country. Moreover, the society remains divided on the "Cyprus problem" and the resulting split in the media environment poses further challenges to countering disinformation and FIMI by increasing susceptibility to bias or objective or critical evaluation of the information circulated by the media, according to local experts.

For Bulgaria the survey respondents describe the level of cooperation between state institutions and non-state actors as relatively low. Mutual cooperation between the state and non-governmental sectors is usually initiated by NGOs and there is no political will to implement their recommendations. Bulgarian NGOs have also initiated bilateral cooperation, including efforts which led to the signing of the Memorandum of Understanding on combating disinformation with the USA. Administrative representatives, representatives of institutions such as Viginum, representatives of the European Commission are invited to organised meetings, but the implementation of the developed recommendations at the administrative level is extremely slow. Experts point to a phenomenon they call "cognitive capture". The anti-European and anti-American narratives to which Bulgarian officials have been exposed over the past 10 years have meant that if they see US involvement on any project, they immediately become suspicious. Raising public awareness regarding FIMI is the domain of EU institutions, NGO's, media and journalists' associations, but no national public administration and educational institutions. In January 2023 the Bulgarian-Romanian Observatory of Digital Media (BROD), a regional hub and part of the European Digital Media Observatory (EDMO) was established by a decision of the European Commission. In March 2021 the AFP Proveri – the Bulgarian component of Agence France-Presse (AFP) international fact-checking initiative was established. This is a unique initiative due to the

cooperation with Meta as part of its global Third-Party Fact-Checking Program to investigate viral disinformation across Facebook, Instagram, and WhatsApp. Another important fact-checking institution is Factcheck. bg, led by the Association of European Journalists-Bulgaria (AEJ-Bulgaria), which is a non-profit association and member of the International Association of European Journalists (www.aej.org). The aim is to bring together journalists and independent national associations in over 20 European countries. Also worth mentioning is the only initiative run by a public media organisation, the BNR Factcheck, established by Bulgarian National Radio and supported by the competencies within BROD. All the above fact-checking initiatives had a start in 2021. Furthermore, various NGOs and other organisations in Bulgaria are tackling disinformation. A non-exhaustive list includes the Bulgarian Coalition against Disinformation and the Center for the Study of Democracy, which is a member of the BROD consortium. Bulgaria has taken part in several media literacy initiatives. They are often sponsored by private enterprises like Poynter or like-minded embassies (British, US, French and German). The Media Literacy Coalition is a network organisation, which works to integrate media literacy fully into the educational process and to increase media literacy in society, by building cooperation with governmental and non-governmental organisations and institutions relevant to education and media literacy in Bulgaria. Media literacy initiatives are often centred on schools and target young people.

In Romania the level of cooperation between state institutions and civil society is rather low. There was no real public debate on how the state should tackle disinformation and conduct strategic communications. Big newspapers and outlets receive a lot of funding from political parties often in a covert manner, which affects their independence. Despite their relatively low trust in information coming from social media, Romanians still use Facebook as their main source of information. However, Romanians were more than eight times less likely (3%) to view Russia as a strategic ally after the invasion, compared to Bulgarians (26%). According to the GLOBSEC vulnerability towards foreign influence index, the overall score of Romania is 29/100. This is a high level of resilience, especially compared to countries in the Western Balkans. Misreport, a fact-checking newsletter, relies on journalistic methods, which sets it apart from other organisations. Based on developing their own workflow - a combination of media literacy, OSINT and fact-checking tools, they do investigative work on disinformation. The purpose is to map the tactics of placing disinformation in the online space. Misreport decides on the validity of an incident based on the popularity and scale of the spread of false information, or when it notices a new trend/tactic. The next step is to analyse the reasons for such popularity. There are successful initiatives on implementing media literacy into the educational system. The Center for Independent Journalism together with other organisations is running a media literacy project. It consisted of training the teachers, so that they could teach the children. However, the rate of progress is slow, as the Center can train only a few hundred teachers per year. Regarding the school curriculum, media literacy has been included into it. A strong point in Romania is the high level of public trust in civil society. This creates capital for the implementation of many grassroots initiatives to counter disinformation in Romania, like the mentioned Bulgarian-Romanian Observatory of Digital Media (BROD).

By pooling resources and expertise across various sectors, Spain has made strides toward building a more resilient information ecosystem. Moreover, participatory approaches involving citizens in media literacy programs can further enhance community cohesion. Spain proposed a law in 2019 with the aim of protecting the media sphere before the elections, which was adopted in 2020 as a ministerial order PCM/1030/2020. The Procedure also assumed the collaboration of the private sector and civil society, recognising that their participation is essential to counter disinformation campaigns. That assumption materialised in 2022 with the establishment of the Forum against Disinformation Campaigns. The Forum

gathered experts from different civil society sectors, including academia, media or think-tanks to coordinate with the state institutions through different working groups focused on fighting disinformation. Additionally, regulation provides for charging media organisations with (partial) responsibility for developing media literacy skills among the Spanish citizens. According to the Report written by the Forum Against Disinformation Campaigns, what is missing in terms of institutional capacities is the collaboration between universities (and other civil society actors) and local governments in the area of disinformation. In Spain attacks on journalists during protests and harassment of journalists by the supporters of far-right ideology in social media were noticed. The challenge for both media and its consumers is that according to the Reuters Digital News Report, Spain has one of the highest levels of "perceived news outlet polarization". When it comes to social coherence, an important challenge is the division of Spain into 17 parts which constitute autonomous communities with some expressing separatists ambitions. Catalonia is the main case in point. In 2017 its autonomous government organised an illegal independent referendum, which was met with "heavy police crackdown". One of the most important non-profit organisation fighting disinformation in Spain is Maldita.es. It is focusing mostly on fact-checking through operations performed by the team of experts from multiple fields, such as: scientific disinformation, tech awareness, data and transparency, and scam-debunking. Its engineers are working on AI-based tools that could increase efficiency of tracking and debunking disinformation. Part of their work includes monitoring WhatsApp through the number where everyone can reach out after seeing a piece of information they are not sure is correct. Another important organisation is Iberifier. It was launched in 2021 and tackles disinformation in both Portugal and Spain through cooperation with around 90 researchers specialising in digital communication, disinformation, computing and strategic analyses.

5.5. Conclusions

The increasing prevalence of echo chambers and selective exposure to media can lead to a populace that is less informed and more susceptible to disinformation. For instance, the rising influence of especially of far-right groups and the proliferation of conspiracy theories have highlighted the vulnerabilities within a society that, while generally resilient, is not immune to the polarizing effects of misinformation. Engaging with marginalized communities, addressing their specific vulnerabilities, and creating tailored media literacy programs can help bridge the gaps that division often creates. Moreover, transparency in communication and the establishment of trust between citizens and institutions will be pivotal in overcoming the scepticism that often arises in polarized environments.

The interplay between societal resilience, social cohesion, and media literacy is complex and multifaceted. While NGOs play a vital role in promoting these elements, the effectiveness of their efforts is contingent upon the dynamics of cooperation with governmental bodies and the media. Societies can bolster their resilience against foreign influence and misinformation by prioritizing collaborative initiatives and fostering an environment of trust and inclusion. As the challenges of polarization and fragmentation continue to evolve, it is imperative for stakeholders to remain adaptable and proactive in their approaches, ensuring that the foundations of social cohesion and media literacy are continually strengthened. Ultimately, a robust and resilient society will be one that actively engages its citizens, cultivates critical thinking, and works collectively to navigate the intricacies of the modern information landscape.

Part 6 – Lessons-learned from Ukraine

Filip Bryjka

Ukraine is one of the most experienced countries in the world in the fight against Russian disinformation campaigns. Over the last decade, Ukraine has faced both Russian actions oriented towards interference in political processes, destabilisation, discrediting in the international arena, as well as information operations in support of military action. The Ukrainian experience is extremely valuable for EU countries. The Hybrid CoE and DFRLab report[192] identifies ten best practices for countering disinformation used by Ukraine, based on lessons learned from the country's experience during its hybrid war with Russia from the time of Euromaidan/Revolution of Dignity (late 2013/early 2014) to the 24 February 2022 Russian full-scale invasion of Ukraine. In many cases, Ukrainian approach differs with the approaches developed by the EU and individual Member States.

	Ukraine	EU and its member states
Building a system of resilience against FIMI	Based on state institutions and NGOs	Based on state institutions and NGOs
Coordination	Distributed/decentralised	The drive towards centralisation
Cooperation between civil society and the state	Informal, flexible	Formalised, based on procedures and bureaucracy
Information flow between NGOs and government	Two-way	One-way
FIMI incident response approach	Immediate	Dependent on the scale and harmfulness of the incident
Detection and analysis methods	Differentiated	Drive towards standardisation
Organisation of teams	Mass (involving informal groups of volunteers)	Small, specialised analytical teams
Perception of duplication of tasks (overlapping)	Positive	Negative
Readiness to use countermeasures that impose costs (e.g. sanctions, blockades, naming and shaming, putting public pressure on propagandists) on the adversary	High	Low
Use of satire and parody	High	Low

Source: own study based on J. Kalenský, R. Osadchuk, *How Ukraine fights Russian disinformation: Beehive vs mammoth*, Hybrid CoE Research Report 11, January 2024.

6.1. Systemic approach to detection and response to FIMI

Building a robust and solid system for monitoring the information space and responding rapidly to disinformation campaigns through debunking, refuting lies and other proactive measures. According to Ukrainian practitioners, this is fundamental to state resilience to

[192] See: J. Kalenský, R. Osadchuk, *How Ukraine fights Russian disinformation: Beehive vs mammoth*, Hybrid CoE Research Report 11, January 2024.

FIMI. In doing so, Ukrainians emphasise that speed of response is key, rather than considering whether it is appropriate to take action at all. This approach, differs to the philosophy of the EU and individual member states. According to Ukraine, it is speed that makes debunking work. Moreover, keeping a database of debunked cases makes it easier to respond to further (including new) narrative lines[193]. In doing so, they also draw attention to the repetitiveness of their own message, which cannot be limited to one-off debunking, or naming and shaming. Just as „a lie repeated a thousand times becomes the truth" (which is what disinformers exploit), the truth must be repeated in order to perpetuate itself in society.

6.2. Institutional capacity

Inter-institutional complementarity (and even overlapping or duplication of tasks) is an advantage and should not be seen as a mistake. Each relevant state and military institution should have its own team for monitoring and analysis of the information space, using its own methods of detection and analysis. It sharply contrasts with the approach of the EU and Member States seeking standardisation (based on DISARM-STIX, ABCDE frameworks). According to Ukrainian experts, diversity is an asset because it increases the independence and creativity of entities and individual actors. The dispersion of competences also increases their resilience to disruptions, such as cyber attacks (e.g. DDoS). Even when one institution is blocked, others can continue to operate. In Ukraine, situational awareness is provided primarily by two institutions created by the Ukrainian government in March 2021: Center for Countering Disinformation (CCD) [within the National Security and Defence Council] and the Centre for Strategic Communications (CSC) [within the Ministry of Culture and Information Policy], alongside monitoring work conducted by various NGOs (among others StopFake, Detector Media, Ukrainian Crisis Media Centre, Internews, and Texty). There are at least two unifying forces coordinating counter disinformation efforts under the umbrella of the NDI Disinformation Hub and in cooperation with the CSC communicating with civil society from its inception, understanding the immense importance of the expertise concentrated in the NGO sector. However, this coordination is informal in nature. It is „the ecosystem of people dealing with Russian disinformation was created a while ago, and it became a self-coordinating group to which people added trusted contacts"[194].

The significant human and financial resources allocated by numerous institutions to countering FIMI are crucial. Indeed, limiting them will lead to inefficiency and ineffectiveness in the system. Underfunding and insufficient human resources are a problem for many teams analysing FIMI or responsible for StratCom in EU countries. The Ukrainians point to hundreds of people involved in combating disinformation in Ukraine but do not specify the numbers. In doing so, however, they also take into account volunteers (so-called 'elves' as those in the Baltic states) acting alone or in small groups as volunteers.

6.3. Cooperation between state and non-state entities

The centre of gravity of the counter FIMI system must be based on civil society ('information warriors') and not rely only on the state administration, which is unable to detect and respond effectively to FIMI at local and national level at the same time. Bottom-up initiatives with their own communication channels play an important role. „Cooperation between civil society and government was often flexible and informal, allowing it to focus on specific, organic problem-solving rather than the creation of formal and systematic procedures for collaboration. It is built on the principle of horizontal cooperation, whereby partners could amplify each other's work by sharing their expertise and findings, or through joint

[193] Ibidem, p. 10-13, 16.
[194] Ibidem, p. 18.

programmes, training, and problem-solving"[195]. Importantly, the flow of information between state and NGOs is two-way. Thanks to this model of state-NGOs cooperation, the detection of disinformation is rapid, enabling an immediate response. As the authors of the report point out „these activities involved individual activists as well as civil society groups and private businesses. Some were loosely connected, while others were more organized as a form of "territorial defence" for the information space. Regardless of their background or organizational structure, they take on a number of tasks, including debunking false information and disseminating truthful information, calling out Russian and pro-Russian voices, and monitoring the information space, with some even engaging in sophisticated cyberattacks against targets in Russia"[196].

6.4. Building reslience and response capabilites

Contingency plans must be in place for times of crisis and war (including alternate communication channels, additional infrastructure and teams capable of immediate crisis engagement). Communication channels must be tailored to the audience to reach them easily and effectively (e.g. social media). Audiences cannot be counted on to find their way to receive messages from the government. Starting these activities already after a conflict has erupted will be more difficult to do. Ukrainian government bodies have started to develope such a plan in summer 2021 but these preparations stepped up as intelligence sources, civil society monitoring, and media reporting revealed increasing signs of an attack. To confront such a problem, it was necessary to plan not just general contingency procedures, such as splitting the office into multiple groups in different regions, but also specific prepared messages and instruments that could be deployed at short notice. This preparation included informing Ukrainian society of the impending danger. Government officials prepared materials on what people should do in case of an emergency[197]. The Ukrainian government established "United News telethon", a joint effort of various national channels that started broadcasting on 24 February 2022. The channel provided verified information, serving as a crucial source for the Ukrainian public at the beginning of the invasion. Awareness of an impending conflict should also prompt us to prepare specific material in response to anticipated information operations by the adversary. Indeed, making certain intelligence information public[198] (such as the actions of US intelligence agencies revealing Russia's preparations for war, or 'false flag operations' designed to provide a pretext for invasion) enhances our ability to pre-bunking.

We cannot limit ourselves solely to defence and building resilience. To effectively counter FIMI, it is also necessary to have measures to punish the adversary that impose costs on them, influence their behaviour and limit their ability to conduct hostile actions. Imposing sanctions, blocking domains, naming and shaming are often controversial and questionable in the EU for fear of censorship and violation of freedom of expression. In 2014, Ukraine banned Russian state TV channels. In 2017, Petro Poroshenko's administration blocked access to Russian social media VKontakte and Odnoklassniki, to a Russian mail provider and search engine, and to several pseudo-media sites; this measure was later extended by Volodymyr Zelensky. In 2021, Zelensky's administration banned TV channels plus their information ecosystem (websites, social media channels, direct messaging platform channels), including those that did not directly belong to the Russian state but still spread the same messages[199]. These

[195] Ibidem, p. 21-22.
[196] Ibidem, p. 15.
[197] Ibidem, p. 24.
[198] Jay Paxton, *Operationalizing Intelligence. Shaping the Information Environment and Galvanizing Western Action Against Russia*, „The Three Swords", no. 38, 2022, p. 12-17.
[199] J. Kalenský, R. Osadchuk, *How Ukraine fights*...op.cit., p. 27.

included channels belonging to pro-Kremlin oligarch Viktor Medvedchuk. After the invasion, cooperation with the private sector played an important role. Google has blocked 170 YouTube channels which were violeting Ukrainian criminal code. In a special form delivered to Ukrainian government bodies indicating which law was violated by a channel[200]. Considering bans and blocking domains seemt to be the most extreme option, there are also othe countermeasures imposing costs on adversary, such as naming and shaming. In 2022, a number of Ukrainian ministries and state services, including Military Intelligence and the SSU, published a joint statement on "The protection of Ukraine's information space from Russian hostile Telegram channels" reavling to the public a list of 100 such channels channels connected to Russia[201]. The CCD, in collaboration with other state institutions, later created a blacklist of "information terrorist" Telegram channels[202]. They also compiled a list of international influencers who amplify Russian propaganda[203]. This activity did not come from the government alone. The Institute of Mass Information released a blacklist of people spreading genocidal Russian rhetoric[204]. Vox Ukraine created a database of Russian propaganda appearing in European outlets[205].

Responding to disinformation with humour (including irony, satire, jokes, memes) allows you to reach a wider audience, improves the morale of your own society and undermines the reputation of your opponent, with positive results. The NAFO fellas phenomenon is an example of this[206]. Humorous content is more attractive and goes viral more often. It allows you to reach audiences outside of your usual filter bubble. It helps to discredit, ridicule and mock the enemy. It undermines the credibility of the Kremlin and its propaganda channels. Satirical memes are more likely to be liked by the audience and shared. It also helps to gain the sympathy of neutral audiences. The effectiveness of this tactic, moreover, is well known and exploited by disinformes.

Actions are more important than words. No debunking or strategic communication is as effective as real action. The Ukrainian military operation in the Kursk region on Russian territory in the mid 2024 became a serious problem for Kremlin propaganda and a very effective tool for countering it. The inhabitants of the region, deprived of any assistance from the state, saw first-hand how they were being lied to. Not giving credence to the government's assurances of a 'stable situation', 'organising the evacuation of the population', or 'providing

---

[200] Ibidem, p. 28.
[201] *100 Russian Telegram Channels That Mimic Ukrainian Ones*, Centre for Strategic Communication and Information Security, 2022, https://spravdi.gov.ua/en/100-russian-telegram-channels-that-mimic-ukrainian-ones/
[202] *CCD Announces an Updated List of Infoterrorist Channels Operating in Ukraine*, Center for Countering Disinformation, 2023, https://cpd.gov.ua/en/warnings/ccd-announces-an-updated-list-of-infoterrorist-channels-operating-in-ukraine/
[203] Спікери, Які Просувають Співзвучні Російській Пропаганді Наративи [Speakers who promote narratives consistent with Russian propaganda], Center for Countering Disinformation, 2022. https://web.archive.org/web/20220801015336/https://cpd.gov.ua/reports/. In contrast to the blacklists, the CSC also created "whitelists" of sources that could be trusted, including Ukrainian government channels.
[204] Нестеренко, Альона, Роман Головенко, and Оксана Романюк. «Ядерний Удар По Вінниці Та Гулаг Для Запорізьких Учителів. Геноцидна Риторика Російської Пропаганди [A Nuclear Attack on Vinnytsia and the Gulag for Zaporizhzhia Teachers. The Genocidal Rhetoric of Russian Propaganda]." Інститут масової інформації, 2022. https://imi.org.ua/monitorings/yadernyj-udar-po-vinnytsi-ta-gulag-dlya-zaporizkyh-vchyteliv-genotsydna-rytoryka-rosijskoyi-i48786.
[205] VoxCheck Team. "Propaganda Diary 2022–2023: Voxcheck Presents the Database of Russian Propaganda in the European Mass Media." Vox Ukraine, 2023. https://voxukraine.org/en/propaganda-diary-2022-2023-voxcheck-presents-the-database-of-russian-propaganda-in-the-european-mass-media.
[206] See: Keir Giles, *Humour in online information warfare: Case study on Russia's war on Ukraine*, Hybrid CoE, November 2023.

humanitarian aid' – they spared no criticism of the authorities in material published on social media[207].

In the case of Ukraine, pro-Russian sympathies were largely eliminated after Russian rockets and artillery began raining down on Ukrainian cities. Images of Russian war crimes committed in Ukraine consolidated the West on the side of Ukraine, but did not change the attitudes of societies in the Global South. Russia was denying its war crime and questioned its responsibility. An example of this is the falsification of the public's perception of the Bucha crime. Despite unequivocal evidence, Russian disinformation channels claimed that massacre was staged by the Ukrainians.

6.5. Conclusions

The West should learn from Ukraine and try to catch up with it in the fight against FIMI. According to Ukraine, the EU countries are doing insufficiently in countering Russian disinformation, this especially concerns the low willingness to apply countermeasures imposing costs on Russia (blocking disinformation channels). At the same time, Ukraine asks the West for support and cooperation in the information warfare, through the creation of joint task forces.

There should be no illusion that information warfare will end or be reduced. Even if the warfare is ended, we will still have competition in the information sphere. It is a war that cannot be won, no winner or loser can be identified, only its harmful effects can be mitigated. There is no theory of victory in information warfare. The process exploits new events from an endless news cycle, applying tried and tested propaganda techniques to manipulate facts in narrative weapons. The adversary develops its TTPs and adapts to our countermeasures. The potential range of tools, topics, and platforms is constantly growing, making the cycle indefinite while deepening it.

[207] EUvsDisinfo, *The Kursk Problem*, „Disinformation Review", https://euvsdisinfo.eu/the-kursk-problem/, 22.08.2024